

КОМИТЕТ ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ ВОЛГОГРАДСКОЙ
ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «КОТОВСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»
(ГБПОУ «КОТОВСКИЙ ПРОМЫШЛЕННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»)

УТВЕРЖДАЮ

Зам. директора по УР

З.Ф. Дьякова

« 5 » 02 2020 г.



**ЭЛЕКТРОННОЙ КУРС ПО ТЕМЕ «ДИАГНОСТИКА
НЕИСПРАВНОСТЕЙ СЕТЕВОЙ ИНФРАСТРУКТУРЫ»**

МДК 03.01 Эксплуатация объектов сетевой инфраструктуры
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

09.02.02 Компьютерные сети

Форма обучения **ОЧНАЯ**

Котово,
2020

Электронный курс по теме «Диагностика неисправностей сетевой инфраструктуры» по МДК 03.01 Эксплуатация объектов сетевой инфраструктуры профессионального модуля ПМ.03 Эксплуатация объектов сетевой инфраструктуры специальности 09.02.02 Компьютерные сети.
Форма обучения очная

Организация-разработчик: Государственное профессиональное образовательное учреждение «Котовский промышленно-экономический техникум» бюджетное

Разработчики:

Трунова Людмила Владимировна, председатель ЦМО, преподаватель профессиональных дисциплин

РАССМОТРЕНО

На заседании ЦМО МЕН и ВТ

Протокол № 4 от 3.02 2020 г.

Председатель ЦМО Юрид / Трунова Л.В.

РЕКОМЕНДОВАНО

Научно-методический совет

Заключение № 6 от 5.02 2020 г.

Председатель методического совета ЗФ З.Ф.Дьякова

СОДЕРЖАНИЕ

Пояснительная записка	4
Содержание электронного курса по теме « Диагностика неисправностей сетевой инфраструктуры»	4
Средства мониторинга и анализа сетей	4
Принципы локализации неисправностей	7
Нагрузочное тестирование сети.....	12
Программные средства диагностики	24
Номенклатура и особенности работы тест-программ	29
Диагностика неисправностей средств сетевых коммуникаций.....	35
Введение в диагностику кабельных систем	35
Оборудование для проверки кабельных систем.....	42
Лабораторная работа	48
Порядок выполнения работ	49
Контрольные вопросы.....	55
Контрольный тест.....	56
СПИСОК ЛИТЕРАТУРЫ	58
ПРИЛОЖЕНИЕ А	61
ПРИЛОЖЕНИЕ Б.....	62
ПРИЛОЖЕНИЕ В	63
ПРИЛОЖЕНИЕ Г	64

Пояснительная записка

Электронный курс разработан в соответствии с требованиями государственного стандарта по курсу «Компьютерные сети». Оно предназначено, в первую очередь, для студентов техникума всех форм обучения, в чьи учебные планы включен названный курс, и может быть использовано как в качестве материала для семинарских занятий, так и для самостоятельного изучения профессионального модуля ПМ 03 «Эксплуатация объектов сетевой инфраструктуры» МДК 03.01 «Эксплуатация объектов сетевой инфраструктуры» по теме «Диагностика сетевой инфраструктуры»

В электронный курс входят:

- Лекции по данной теме.
- Инструкционная карта лабораторной работы.
- Контрольные вопросы.
- Контрольный тест (после прохождения теста, в которой дается по три попытки на один вопрос выводится результат в процентах).
- Учебное видео

Содержание электронного курса по теме «Диагностика неисправностей сетевой инфраструктуры»

Настоящее учебное пособие в электронном формате адресовано студентам старших курсов, обучающихся по специальности 09.02.02 «Компьютерные сети».

Средства мониторинга и анализа сетей

Постоянный контроль функционирования ЛВС, составляющей основу любой корпоративной сети, необходим для поддержания ее в работоспособном состоянии. Контроль — это необходимый первый этап, который должен выполняться при управлении сетью. Вследствие важности этой функции ее часто отделяют от других функций систем управления и реализуют специальными средствами. Такое разделение функций контроля и собственно

управления полезно для небольших и средних сетей, для которых установка интегрированной системы управления экономически нецелесообразна. Использование автономных средств контроля помогает администратору сети выявить проблемные участки и устройства сети, а их отключение или реконфигурацию он может выполнять в этом случае вручную.

Процесс контроля работы сети обычно разделяют на два этапа: мониторинг и анализ.

На этапе мониторинга выполняется более простая процедура — процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов и т. п.

Далее выполняется этап анализа, под которым понимается более сложный и интеллектуальный процесс осмысления собранной на этапе мониторинга информации, сопоставления ее с данными, полученными ранее, и выработки предположений о возможных причинах замедленной или ненадежной работы сети.

Задачи мониторинга решаются с помощью программных и аппаратных измерителей, тестеров, сетевых анализаторов, встроенных средств мониторинга коммуникационных устройств, а также Агентов систем управления. Задача анализа требует более активного участия человека и использования таких сложных средств, как экспертные системы, аккумулирующие практический опыт многих сетевых специалистов.

Все многообразие средств мониторинга и анализа сети подразделяется на следующие группы.

1. Агенты систем управления, поддерживающие функции одной из стандартных MIB и поставляющие информацию по протоколу SNMP или CMIP. Для получения данных от Агентов обычно требуется наличие системы управления, собирающей данные от Агентов в автоматическом режиме.

2. Встроенные системы диагностики и управления, выполняемые в виде программно-аппаратных модулей, встраиваемых в коммуникационное оборудование, а также в виде программных модулей, встроенных в ОС.

3. Анализаторы протоколов, представляющие собой программные или аппаратно-программные системы, которые выполняют функции мониторинга и анализа трафика в сетях. Анализаторы протоколов предоставляют возможность собирать данные о работе протоколов всех уровней сети и в большинстве случаев способны производить генерацию тестового сетевого трафика. Анализаторы протоколов имеют большой буфер для сбора пакетов, что позволяет им быстро локализовать причину сбоя в сети, такую как перегрузку сервера и (или) исчезновение пакетов транспортного уровня.

4. Экспертные системы, аккумулирующие знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах их устранения. Экспертные системы часто реализуются в виде отдельных подсистем различных средств мониторинга и анализа сетей: систем управления сетями, анализаторов протоколов, сетевых анализаторов. Простейшим вариантом экспертной системы является контекстно-зависимая система помощи. Более сложные экспертные системы представляют собой, так называемые базы знаний, обладающие элементами искусственного интеллекта. Примерами таких систем являются экспертные системы, встроенные в систему управления Spectrum компании Cabletron и анализатора протоколов Sniffer компании Network General. Работа экспертных систем заключается в анализе большого числа событий для выдачи пользователю краткого диагноза о причине неисправности сети.

Анализатор может захватывать и декодировать до нескольких десятков протоколов, применяемых в сетях, ставить логические условия для захвата отдельных пакетов и выполнять полное декодирование захваченных пакетов, т.е. показывать в удобной для специалиста форме вложенность пакетов протоколов разных уровней друг в друга (инкапсуляцию) с расшифровкой содержания отдельных полей каждого пакета.

Кроме того, анализатор сетевых протоколов может использоваться для решения следующих задач:

- изучение работы сети и локализация трудноразрешимых проблем;
- обнаружение и идентификация несанкционированного ПО;
- получение базовых моделей трафика и метрики утилизации сети (здесь термин «метрика утилизации» показывает степень загрузки сети в определенном географическом месте и в определенное время);
- идентификация неиспользуемых протоколов для удаления их из сети;
- генерация трафика для испытания на вторжение в целях проверки системы защиты;
- работа с системами обнаружения вторжений;
- прослушивание трафика, т.е. локализация несанкционированного трафика с использованием, например, беспроводных точек доступа.

5. Многофункциональные портативные устройства анализа и диагностики. В связи с развитием технологии больших интегральных схем появилась возможность производства портативных приборов, которые совмещали бы функции нескольких устройств: кабельных сканеров, сетевых мониторов и анализаторов протоколов.

6. Оборудование для диагностики и сертификации кабельных систем, которое условно подразделяется на четыре основные группы: сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

Принципы локализации неисправностей

Диагностика сети — это измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы пользователей). Диагностикой сети является, в частности, измерение числа ошибок передачи данных, степени загрузки ресурсов и пр. Диагностика бывает двух типов: упреждающая и

реактивная. Основная цель упреждающей диагностики — предотвращение сбоев в работе сети. Упреждающая диагностика должна проводиться в процессе эксплуатации сети ежедневно.

Реактивная диагностика выполняется, когда в сети уже произошел сбой и требуется быстро локализовать источник и выявить причину.

Тестирование сети — это процесс активного воздействия на сеть в целях проверки ее работоспособности и определения потенциальных возможностей по передаче сетевого трафика. Тестирование, в отличие от диагностики, подразумевает отсутствие в сети работающих пользователей. Оно может применяться для решения следующих задач:

- проверка соответствия качества СКС требованиям стандартов;
- определение максимальной пропускной способности сети;
- проверка устойчивости работы конкретных сетевых устройств при различных уровнях нагрузок и различных типах сетевого трафика.

В основе методов разработки тестовых и диагностических программ локализации неисправностей сети лежат следующие принципы.

1. Зависимость от модели OSI. Для проведения диагностики сети администратор должен ясно представлять себе способы размещения сетевых узлов и методы их взаимодействия друг с другом. Основу этих сведений составляют протоколы. Именно знание протоколов лежит в основе успешных действий по анализу и диагностике сетей. Протоколы являются основой:

- подключения к сети новых узлов;
- разделения потока данных на отдельные пакеты;
- обмена пакетами между устройствами в сети.

Эффективной следует признать только ту методологию диагностики сети, которая зеркально отражает модель OSI: анализ начинается с самого нижнего уровня (физического) и, при необходимости, поэтапно продолжается до самого верхнего уровня — уровня приложений. Например, нет смысла начинать поиск низкой производительности сети на уровне приложений файлового сервера,

если в физическом сегменте Ethernet клиента наблюдается чрезмерно большое число ошибок CRC (Cyclic Redundancy Code — избыточный циклический код).

Большинство реализаций конкретных сетей не совпадает с моделью OSI в точности, но в любой такой реализации функции, описанные моделью OSI, по крайней мере, принимаются в расчет. Ценность модели OSI в качестве инструмента поиска неисправностей заключается в описании принципов функционирования сети. Другими словами, имея точное представление о том, что делает сценарий, можно точно локализовать проблему

2. Декомпозиция сетевой проблемы. Даже в простом случае сети с двумя узлами существует много аппаратуры и параметров ПО, взаимосвязь между которыми может значительно влиять на эффективность работы сети. Обычно подход к такой сложной проблеме должен начинаться с декомпозиции общей проблемы на более мелкие части и так далее, до нахождения первоисточников проблемы, а затем уже должен выполняться систематический и логический план удаления возможных причин, пока не будет достигнуто ее решение.

3. Выбор правильного инструмента диагностики. Есть существенные различия в способах измерения производительности у разных инструментов тестирования, при этом важно их взаимодействие с тестируемой системой. Существует два класса тестовых систем: генераторы трафика и генераторы транзакций. Генераторы трафика являются источником огромного числа пакетов, которые могут как соответствовать трафику реального сетевого стека, так и отличаться от него. Генераторы транзакций, как минимум, отсылают и принимают реальные транзакции через полноценный работающий сетевой стек OSI. Главное их отличие от генераторов трафика заключается в том, что они реализуют настоящий сетевой стек, в том числе и на прикладном уровне.

При выборе правильного инструмента диагностики ключевым является вопрос: нужна ли для тестирования данной системы работа на четвертом (транспортном) и более высоких уровнях OSI? Устройствам, которые взаимодействуют с потоками транспортного уровня, таким как межсетевые

экраны и распределители нагрузки, требуется генератор транзакций. Поскольку эти системы взаимодействуют с потоком транспортного уровня, то и генерировать его нужно соответствующим образом. Такая тестируемая система может вступать во взаимодействие с приложением, содержащим динамический контент. В этом случае искусственный трафик четвертого уровня (и более высокого) не будет должным образом обработан тестируемой системой, так как имитационный трафик предполагает наличие ожидаемых откликов на запросы.

4. Принцип «сверху вниз». Поиск неисправностей следует проводить «снизу вверх», т.е. начиная с физического уровня и заканчивая уровнем приложений. Например, плохая кабельная сеть является причиной 90 % всех сетевых проблем, поэтому так важно начинать диагностику сети именно с физического уровня, используя для этого качественный кабельный тестер. Такие приборы работают быстро и обеспечивают высокую точность. Однако поиск оставшихся 10% ошибок потребует 90% общего времени на восстановление работоспособности сети.

Каждому уровню модели OSI свойственны свои характерные проблемы, обнаруживаемые при сбоях в сети именно на этих уровнях. В таблице 1 представлены наиболее характерные из них.

5. Документирование сети. Квалифицированный сетевой аналитик всегда начинает анализ сети с полного понимания текущей сетевой среды, что подразумевает документирование сетевой топологии, прикладных программ и используемых протоколов. Трудно переоценить важность точной и подробной документации для сети. Обычно сетевая документация содержится в разрозненных документах, причем даже собранные воедино они не позволяют получить полную картину сети.

Таблица 1 – Проблемы, обнаруживаемые при сбоях в сети

Наименование уровня	Возможные сетевые проблемы на соответствующем уровне
------------------------	--

Уровень приложений	Зацикливание (перекрытие) запросов на чтение (запись) файлов. Долгий поиск ресурсов, замедленная обработка данных клиентом (сервером). Плохое заполнение пакетов данными. Низкая пропускная способность между хостами сети
Представительский уровень	Несовместимость протоколов. Некорректные сведения в базе данных MIB протокола SNMP. Замена кодовых таблиц ASCII на EBCDIC
Сеансовый уровень	Согласование MTU блока и буфера. Поиск и регистрация ресурсов по логическим именам. Повторная установка соединений
Транспортный уровень	Повторные пересылки. Избыточная фрагментация или ее отбрасывание. Превышение длины посылаемого сегмента размера скользящего окна
Сетевой уровень	Ошибки CRC. Проблемы маршрутизации (задержки, отбрасывание пакетов, несогласованность MTU). «Широковещательные» штормы
Канальный уровень	Ошибки CRC. Конфликты и фрагментация кадров. Ошибки линии и пакета. Очистка кольца и аварийная сигнализация. Задержки, отбрасывание пакетов, искажение данных в коммутаторах и мостах. «Штормы»
Физический уровень	Неисправности и ошибки СКС (соединители, расщепление пары, обрывы, короткое замыкание (КЗ), некорректная длина линии). Отказы портов, концентраторов, внешние высокочастотные помехи.

Насыщение полосы пропускания наблюдения за работой сети. Очень важна хорошая регистрация ежеминутных изменений сети, но без постоянного обновления всего комплекта документации.

Точная и понятная документация для сети, отражающая все изменения в сети, позволяет успешно управлять оборудованием и эффективно проводить диагностику, причем необходимо заранее выделять рабочее время на поддержание документации на должном уровне.

Не следует подробно отражать на структурной схеме каждый хост в каждом сегменте сети, поскольку редко удастся постоянно поддерживать корректность этих сведений, однако необходимо отразить топологию и все коммуникационное оборудование: коммутаторы, маршрутизаторы, серверы, шлюзы и средства защиты сетей. При этом достаточно упрощенных

изображений, подчиняющихся общей системе условных обозначений (например, всегда маршрутизатор изображать восьмиугольником, а коммутатор квадратом и т.д.). Внутри этих фигур можно поместить полезную информацию об оборудовании, а рядом — показать IP-адрес, дополненный маской подсети.

6. Входное тестирование. Множество проблем в сети можно избежать, если качественно провести тестирование сети на этапе ее приемки у системного интегратора. Прежде всего — это относится к сертификации кабельного хозяйства на соответствие стандартам и тестированию сетевого оборудования на наличие скрытых дефектов. Правилom хорошего тона для системного интегратора является не только проведение тестирования, но и внесение его данных в паспорт сети, предоставляемый пользователю. Если входное тестирование не проводится, то пользователь может получить сеть со скрытыми дефектами, которые проявятся не сразу, так как на начальных этапах эксплуатации сети нагрузка в ней мала. Дефект может проявиться значительно позже, создав у пользователя впечатление, что он явился следствием каких-то модификаций в сети.

Нагрузочное тестирование сети

Нагрузочное тестирование — это вид диагностики сетевой инфраструктуры, позволяющий получить интегральную оценку качества работы сети и локализовать скрытые дефекты. Нагрузочное тестирование, которое также называют стрессовым тестированием, или имитацией трафика, проводится:

- для получения интегральной оценки качества работы модифицируемой (новой) сети и определения запаса ее производительности;
- выявления скрытых дефектов сетевых адаптеров и драйверов;
- измерения производительности и выявления скрытых дефектов активного сетевого оборудования;
- сравнения эффективности различных сетевых архитектур.

Хост имитатор	Воздействие	Тестируемое
---------------	-------------	-------------

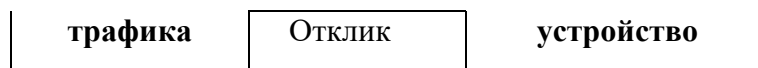


Рисунок 1 – Схема нагрузочного тестирования

Идею нагрузочного тестирования поясняет рисунок 1. хост — имитатор трафика создает в сети диапазон нагрузок с переменной плотностью и составом цифрового потока. Одновременно с этим измеряются скоростные и нагрузочные характеристик сети. Если выясняется, что скорость рабочих станций и пропускная способность сети соответствуют тем значениям, которые ожидаются от сети с данной архитектурой, значит, дефектов нет. Если же какие-то станции работают с низкой скоростью или отключаются от сервера, значит, дефекты есть.

Общие принципы локализации дефектов при проведении нагрузочного тестирования. В качестве основного критерия качества работы сети здесь используется скорость выполнения файловых операций каждым хостом. Этот критерий выбран, прежде всего, потому, что если в каком-либо компоненте рабочей станции есть дефект, то с вероятностью, близкой к 100%, он проявится в низкой скорости выполнения файловых операций. Другая причина заключается в том, что скорость файловых операций не очень сложно измерить. Если скорость мала, то, изменяя режим работы станций, легко определить причину этого.

Рассмотрим несколько простых правил, соблюдая которые, можно избежать отсутствия на хостах дефектов.

1. Если хосты работают с сервером по очереди, то скорость выполнения файловых операций каждой станцией должна быть пропорциональна производительности ее компьютера и сетевой карты. Если на каком-то хосте с «быстрой» сетевой картой файловые операции выполняются медленно, то это предмет для изучения.

2. Если рабочие станции работают с сервером по очереди, то скорость выполнения файловых операций каждой станцией не должна быть существенно меньше теоретической пропускной способности коллизийного домена

(сегмента) сети, в которой станция расположена. Например, если станция расположена в коллизийном домене Ethernet, ее скорость должна быть в диапазоне 800... 1 150 Кбайт/с.

3. Если рабочие станции работают с сервером по очереди, то число ошибок канального уровня, измеренных в процессе работы каждой станции анализатором сетевых протоколов, должно быть равно нулю.

4. Если все станции работают одновременно, то, как бы сильно ни была загружена сеть, не должно быть станций, скорость работы которых близка к нулю или которые отключаются от сервера.

5. Если все станции работают одновременно и при этом увеличивают интенсивность запросов к серверу, то максимальная производительность всех станций не должна быть существенно ниже теоретической пропускной способности сети.

6. Если все станции работают одновременно и при этом увеличивают интенсивность запросов к серверу, то число ошибок (не путать с коллизиями) канального уровня, измеряемых в ходе теста анализатором сетевых протоколов или SNMP-консолью, должно быть близко к нулю и не должно увеличиваться с ростом утилизации сети.

7. Скорость выполнения операций чтения может отличаться от скорости выполнения операций записи не более чем на 10...30%.

При проведении диагностики сети важно выявить стабильно неадекватную реакцию сети на воздействия тестовых приложений. Если неадекватную реакцию сети можно воспроизвести, значит, можно определить и ее причину и локализовать дефект или «узкое место» сети.

Для проведения нагрузочного тестирования применяются разные тестовые приложения, такие как FTest, SelfTest и т. п. Одновременно с этим могут использоваться различные средства анализа работы сети и серверов (анализаторы протоколов, SNMP- консоли, утилиты сетевых ОС).

Перед проведением тестирования на все хосты проверяемых фрагментов сети устанавливается специальное ПО (FTAgent), которое осуществляет

генерацию тестового трафика в соответствии с заданными параметрами. Тестовый трафик создается за счет выполнения файловых операций между Агентами (хостами с установленной программой FTAgent) и каким-либо сервером. Управление работой всех Агентов осуществляется централизованно с одной рабочей станции сети, играющей роль сервера. Агенты выполняют файловые операции с одним общим файлом на сервере либо с индивидуальными файлами на сервере.

Файловые операции — это либо чтение (запись) блока данных фиксированного размера из файла (в файл), либо последовательность операций (файловая транзакция): блокирование файла —> чтение данных из файла -> запись данных в файл —> разблокирование файла. Все файловые операции выполняются в режиме произвольного доступа к файлу.

В ходе выполнения файловых операций Агенты измеряют скоростные и нагрузочные характеристики сети. Скоростные характеристики сети — это скорость выполнения агентами файловых операций с тестовым сервером. Нагрузочные характеристики сети — это производительность, достигнутая Агентами при выполнении файловых операций с тестовым сервером.

Программа FTAgent спроектирована таким образом, что передаваемые ей данные «обходят» кэш-память рабочей станции, на которой она установлена. Это позволяет измерять реальные значения скорости работы сети вместо показателей быстродействия кэш-памяти.

Типы нагрузочных тестов. Проведение нагрузочного тестирования предполагает выполнение нескольких типов тестов. Каждый тест по-разному воздействует на сеть и поэтому диагностирует различные компоненты сети. Типовая последовательность нагрузочных тестов, которая подойдет для большинства случаев, подразумевает выполнение теста:

- FTest by steps в режиме калибровки с нагрузкой только на сеть;
- FTest all stations с нагрузкой только на сеть;
- FTest all stations с нагрузкой на сеть и сервер;

- FTest by steps (нормальный режим) с нагрузкой только на сеть.

Тест FTest by step в режиме калибровки с нагрузкой только на сеть. Обычно нагрузочное тестирование сети целесообразно начинать именно с режима калибровки. В этом режиме все Агенты по очереди выполняют одни и те же файловые операции, с одним тестовым сервером, с одинаковой интенсивностью. Слова «с нагрузкой только на сеть» означают следующее. Параметры теста задаются так, чтобы производительность дисковой системы тестового сервера в ходе выполнения теста не оказывала существенного влияния на измеряемые скоростные характеристики сети.

Цель выполнения теста — локализовать дефекты сети, которые не являются следствием взаимного влияния одних рабочих станций на другие. Это могут быть дефекты активного и (или) пассивного сетевого оборудования, дефекты в системном ПО хостов или сервера, не оптимальные для данной архитектуры сети параметры настройки сетевого оборудования или ПО и т. п. Рекомендуемые параметры теста, которые подойдут для большинства случаев: предлагаемая нагрузка — задается так, чтобы интенсивность, с которой каждый агент будет стараться генерировать трафик, превышала теоретическую пропускную способность коллизионного домена (сегмента) сети, в котором расположен агент, — принять 10 Мбайт/с;

- доля операций чтения — принять 50 %;
- размер файла — принять 64 Кбит;
- размер записи — принять 8 192 байт;
- разделяемый файл и параметр CRC — принять «Нет». Остальные параметры задаются в соответствии с общей логикой работы теста исходя из следующих соображений.

1. Для каждого агента средняя скорость выполнения файловых операций не должна быть существенно меньше теоретической пропускной способности коллизионного домена (сегмента) сети, в котором агент

расположен. В большинстве случаев для сетей Ethernet, Half Duplex это значение должно быть в диапазоне 800... 1 150 Кбайт/с.

2. Для каждого агента измеряемые значения скорости выполнения операций чтения-записи и значения производительности должны быть прямо пропорциональны значению индекса производительности компьютера агента и производительности его сетевой карты.

3. Для каждого агента скорость выполнения операций чтения не должна существенно отличаться от скорости выполнения операций записи. Как правило, скорость выполнения операций чтения немного выше (на 5... 10%), чем скорость выполнения операций записи.

4. Утилизация канала связи (порта коммутатора), измеряемая в процессе работы каждого агента анализатором сетевых протоколов, не должна существенно отличаться от измеряемых каждым агентом значений производительности. Как правило, утилизация канала связи должна быть на 5... 10% выше, чем измеряемое значение производительности.

Число ошибок канального уровня, измеренное в процессе работы каждого агента анализатором сетевых протоколов, должно быть равно нулю.

Для проведения нагрузочного тестирования применяются тестовые приложения FTest и SelFTest. Одновременно с этим могут использоваться различные средства анализа работы сети и серверов (анализаторы протоколов, SNMP-консоли, утилиты сетевых ОС и т.п.).

Тест FTest all stations с нагрузкой только на сеть. Этот тест выполняется только после того, как реакция всех агентов в ходе выполнения теста FTest by steps в режиме калибровки была признана адекватной. В процессе выполнения этого теста все агенты одновременно выполняют одни и те же файловые операции, с одним тестовым сервером, постепенно наращивая их интенсивность.

Цели выполнения теста:

1. локализовать дефекты, которые являются следствием высокой нагрузки в сети и (или) взаимного влияния хостов. Это могут быть дефекты

активного сетевого оборудования, дефекты в системном ПО хостов и (или) сервера, неоптимальные для данной архитектуры сети параметры настройки активного сетевого оборудования или ПО и т. п.;

2. локализовать «узкие места» сети (без учета дисковой системы сервера);

3. измерить общую производительность сети (без учета дисковой системы сервера).

При задании параметров для этого теста необходимо учесть, что минимальная и максимальная предлагаемые нагрузки, а также число шагов тестирования являются взаимосвязанными параметрами. Значения параметров задаются так: на первом шаге теста общая загрузка сети не должна превышать 10% теоретической пропускной способности (ТПС) сети, а на последнем — должна составлять 150...200 % ТПС сети; не менее трех последних шагов теста должны соответствовать нагрузке на сеть, превышающей 100 % ТПС сети, и один шаг выполняется при нагрузке 30...40% ТПС сети. Остальные параметры теста можно принять, как в предыдущем тесте.

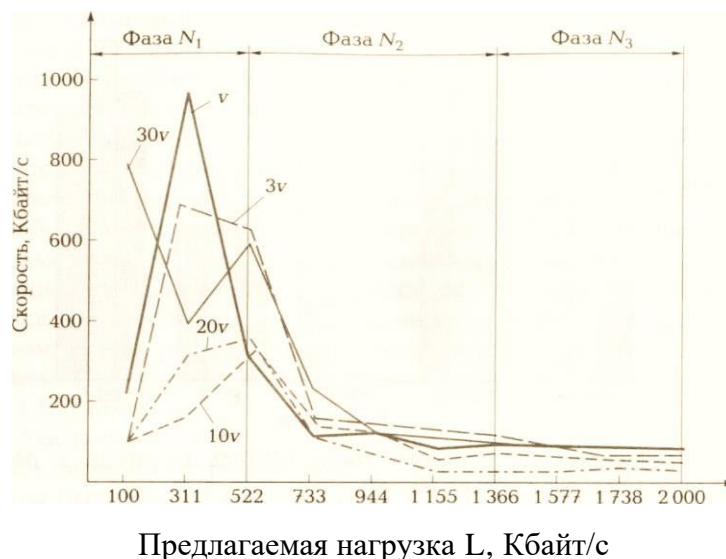


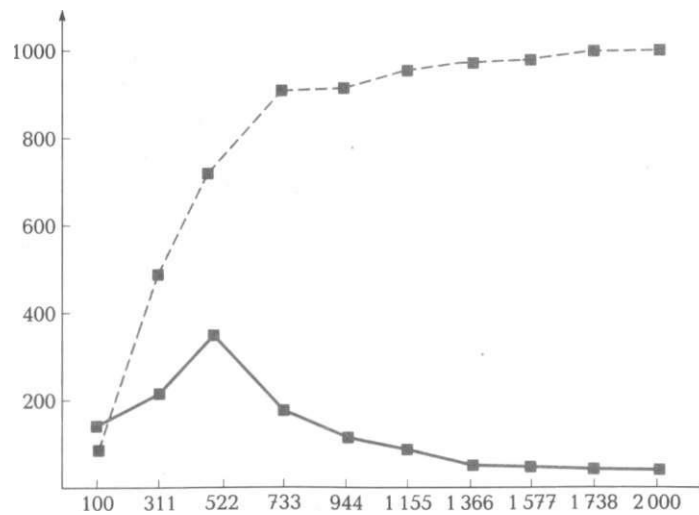
Рисунок 2 – Зависимость скорости чтения от нагрузки на сеть Ethernet

На рисунках 3.3.2, 3.3.3 приведены графики изменения скорости выполнения файловых операций от величины нагрузки на сеть. Здесь v, c^{-1} , — минимальная скорость чтения пакетов Агентами. Штриховая линия на рисунке

3.3.3 показывает зависимость производительности сети от величины предлагаемой нагрузки на сеть, а сплошная — зависимость средней скорости работы агентов от того же аргумента. Анализируя приведенные графики, можно отметить следующую закономерность.

В фазе N_1 в соответствии с рисунком 2, пока предлагаемая нагрузка на сеть низкая, значения скоростей Агентов могут «прыгать». При некоторой нагрузке (здесь это $L_1 = 522$ Кбайт/с) значения скоростей всех Агентов достигают значения, после которого только уменьшаются (фаза N_2). Уменьшение скорости происходит до того момента, когда при определенном значении нагрузки L_2 скорость всех агентов стабилизируется на некотором постоянном, минимальном значении (здесь — на уровне $L_2 = 1\,366$ Кбайт/с). В фазе N_3 значения скоростей стабилизированы на минимальном значении.

Большой разброс скоростей в фазе N_1 объясняется следующими причинами. При низкой нагрузке на сеть производительность канала связи не оказывает существенного влияния на значения скоростей, так как он еще не загружен. Однако сетевые ОС имеют следующую особенность. Чем ниже интенсивность запросов (предлагаемая нагрузка), тем меньше ресурсов сетевая ОС сервера выделяет для обслуживания этих запросов. Этим объясняется большой разброс значений скоростей у разных агентов и то, что скорости могут «прыгать». При этом для некоторых агентов в фазе N_1 можно наблюдать рост значений скорости с увеличением предлагаемой нагрузки, а для некоторых — снижение скорости. Однако усредненное значение скорости по всем агентам, как правило, растет (как видно из рисунка 3.3.3 средняя скорость выполнения операций чтения на первых трех шагах теста растет с 154,7 до 381 Кбайт/с).



Предлагаемая нагрузка I, Кбайт/с

Рисунок 3 – Зависимость производительности сети и средней скорости чтения (записи) всеми агентами от нагрузки на сеть.

Значение нагрузки, равное I_1 , соответствует такой интенсивности запросов, при которой сетевая ОС уже выделяет достаточно ресурсов, но канал связи еще не настолько загружен, чтобы оказывать существенное влияние на скорость выполнения файловых операций. Этим объясняется максимальное значение усредненной по всем агентам скорости на последнем шаге фазы N, (как видно из рисунка 3, максимальное значение усредненной скорости достигается при значении предлагаемой нагрузки, равном 522 Кбайт/с). Интересно, какое значение производительности сети и какое значение утилизации канала связи соответствуют максимальному значению усредненной скорости? Очевидно, что значение утилизации канала связи в этой точке не должно быть выше рекомендуемого для конкретного типа сети. Например, для сети Ethernet на основе разделяемого канала связи рекомендуемое значение — 35...40%. Из рисунка 3 видно, что 522 Кбайт/с предлагаемой нагрузки соответствует производительность, равная 713 Кбайт/с. Учитывая, что тестировалась сеть, состоящая из одного коллизийного домена, это соответствует более чем 60 % утилизации канала связи сети. Следовательно, сервер и канал связи плохо сбалансированы друг с другом по производительности.

Снижение скоростей в фазе N₂ объясняется тем, что производительность канала связи начинает ограничивать скорость выполнения файловых операций. Чем больше предлагаемая нагрузка, тем ниже усредненное значение скорости. Значение L₂ соответствует максимальной производительности тестируемой сети. Таким образом, можно измерить, какова максимальная производительность тестируемой сети. Если производительность компьютеров не хуже производительности канала связи сети, то утилизация канала связи в точке L₂ должна быть 100% (как видно из рисунка 3.3.3, максимальная скорость тестируемой сети равна 1 048 Кбайт/с, что соответствует близкой к 100% утилизации канала связи сети Ethernet).

Фаза N₃ соответствует нагрузке, при которой канал связи или сервер полностью загружены, поэтому скорости постоянны и минимальны. При тестировании коммутируемых сетей значения скоростей могут оставаться постоянными в течение всего теста. Это объясняется фиксированной полосой пропускания, которую имеет каждый агент в коммутируемой сети.

При анализе результатов теста FTest all stations обязательно учитывается архитектура сети. Коммутируемая сеть будет вести себя отлично от сети, построенной на основе разделяемого канала связи. Поэтому основное правило заключается в следующем. Все Агенты, которые находятся в одинаковых условиях и имеют идентичную конфигурацию компьютера, должны работать приблизительно одинаково. Не должно быть агентов, которые без особых на то оснований работают быстрее или медленнее, чем другие. Нужно учитывать следующее:

- а) независимо от нагрузки в сети не должно быть агентов, скорость которых близка к нулю или которые в ходе теста отключаются от сервера;
- б) значение производительности, соответствующее предлагаемой нагрузке 12 не должно быть существенно меньше теоретической пропускной способности сети.

Число ошибок (не коллизий) канального уровня, измеряемое в ходе теста анализатором сетевых протоколов, не должно увеличиваться с ростом предлагаемой нагрузки и должно быть близко к нулю.

Тест FTest all stations с нагрузкой на сеть и сервер. Он выполняется только после того, как в ходе выполнения теста FTest all stations с нагрузкой только на сеть работа всех Агентов признана адекватной. В процессе выполнения теста FTest all stations все Агенты одновременно выполняют одни и те же файловые операции, с одним тестовым сервером, постепенно наращивая их интенсивность.

Единственное отличие данного теста от предыдущего заключается в том, что в данном тесте производительность дисковой системы сервера будет оказывать существенное влияние на скоростные характеристики Агентов.

Цели выполнения этого теста:

- а) определение баланса производительности сервера и производительности остальных компонент сети;
- б) локализация дефектов и «узких мест» на сервере, следствием которых может быть отключение рабочих станций от сервера или крах операционной системы сервера.

Методика задания параметров в данном тесте практически полностью соответствует методике задания параметров в тесте FTest all stations с нагрузкой только на сеть. Более того, все параметры, за исключением параметра «размер файла», рекомендуется принять, как в тесте FTest all stations — с нагрузкой только на сеть. Параметр «размер файла» следует задавать таким, чтобы его значение, как минимум, в два-три раза превышало размер оперативного запоминающего устройства (ОЗУ) на сервере.

При анализе результатов данного теста можно увидеть, что скорость выполнения файловых операций каждым Агентом может резко меняться во всем диапазоне предлагаемых нагрузок. Более того, при повторном выполнении одного и того же теста скорости выполнения файловых операций одним и тем же Агентом могут отличаться друг от друга. Это объясняется, с одной стороны,

взаимным влиянием Агентов при доступе к диску сервера, а с другой — принципом работы дисковой системы сервера. Дело в том, что, обрабатывая запросы от рабочих станций, дисковая система сервера оптимизирует число обращений к диску. В результате этого запросы от рабочих станций обслуживаются не обязательно в том порядке, в каком они поступают на сервер.

В одном случае быстрее могут обслуживаться запросы одного Агента, в другом случае — другого. По этой причине следует анализировать не скорость выполнения файловых операций, а производительность при выполнении файловых операций.

В данном тесте основной интерес представляет суммарное значение производительности по всем Агентам, измеренное на последнем шаге теста. Это значение, как правило, меньше значения производительности, измеренного в ходе выполнения теста FTest all stations с нагрузкой только на сеть. Разница между этими значениями характеризует степень сбалансированности по производительности дисковой системы сервера, с одной стороны, и остальных компонент сети — с другой. Чем меньше разница, тем лучше сбалансированы эти компоненты.

В целях проверки сбалансированности по производительности канала связи и сервера целесообразно с помощью анализатора сетевых протоколов измерить утилизацию канала связи при максимальной нагрузке на сеть. Поскольку производительность дисковой системы сервера, как правило, ниже производительности канала связи сети, в данном тесте именно сервер, скорее всего, будет «узким местом» сети. Чем ближе утилизация канала связи к 100% при максимальном значении предлагаемой нагрузки, тем ближе производительность сервера к производительности канала связи. Чаще всего это значение составляет 50...60 %.

При анализе результатов данного теста следует обратить внимание также на следующее:

- в ходе теста агенты не должны отключаться от сервера;

– производительность Агентов при выполнении ими операций записи не должна быть существенно ниже производительности при выполнении операций чтения.

Максимальная производительность сети должна быть приблизительно равна NU , где N — теоретическая пропускная способность сети; U — утилизация канала связи, выраженная в долях.

Тест FTest by steps (нормальный режим) с нагрузкой только на сеть. Под нормальным режимом понимается выполнение теста в режиме, отличном от режима калибровки. В этом случае на каждом следующем шаге теста автоматически добавляется один агент, т.е. число одновременно работающих Агентов постепенно увеличивается. Данный тест имеет смысл выполнять только в том случае, если в ходе выполнения теста FTest by steps с нагрузкой только на сеть анализатором протоколов или SNMP-консолью было зафиксировано большое число ошибок передачи данных, в то время как в ходе выполнения теста FTest by steps (режим калибровки) ошибок зафиксировано не было. Такая ситуация свидетельствует о том, что ошибки передачи данных являются следствием взаимного влияния агентов.

Измеряя число ошибок передачи данных в ходе выполнения данного теста, можно легко определить, при начале работы какого именно Агента в сети начинают появляться ошибки передачи данных.

Программные средства диагностики

Все ПС диагностики компьютерной сети подразделяются на две группы:

- 1) утилиты, встроенные в операционную систему;
- 2) специализированные диагностические программные продукты, известные как сетевые утилиты.

Утилиты, встроенные в операционную систему, являются исполняемыми операторами, запускаемыми из командной строки ОС. Рассмотрим назначение указанных команд и работу наиболее информативных из них:

`netstat` — отображает статистику протокола и текущих сетевых подключений `tcp/ip`;

`ping` — проверяет наличие связи с указанным узлом;

`tracert` — выводит имена и IP-адреса всех маршрутизаторов, через которые проходят пакеты от локального компьютера к указанному узлу;

`ipconfig` — выводит сведения о текущей конфигурации протокола IP и может осуществлять базовое конфигурирование этого протокола;

`nslookup` — обращается с запросом к DNS-серверу;

`netsh` — показывает различные параметры настроек сети. Получить подробную справку по каждой из этих команд можно, набрав в командной строке соответствующую команду, содержащую в поле операндов символы «/» и «?». Например, справка для встроенной утилиты `ping` будет показана системой после выполнения команды «`ping /?`». Практика показывает, что чаще других используются утилиты `ping` и `tracert`.

Утилита `ping` отправляет запрос указанному узлу сети и фиксирует время между отправкой запроса и получением ответа, т. е. позволяет определить время отклика интересующего сервера. Понятно, что чем оно меньше, тем обмен данными с этим сервером производится быстрее.

Утилита `tracert` выполняет отправку тестового пакета узлу сети, указанному в поле операндов. Утилита отображает информацию обо всех промежуточных маршрутизаторах, через которые прошел пакет на пути к запрошенному узлу, а также минимальное, максимальное и среднее время отклика каждого из них. Это позволяет оценить «расстояние», которое прошел пакет, и на каком участке возникают наибольшие задержки, связанные с передачей данных.

Рассмотрим подробнее смысл результатов, выдаваемых утилитами `ping` и `tracert`. Отсутствие отклика от удаленного сервера на введенную команду `ping` или `tracert` может свидетельствовать о том, что сервер в данный момент недоступен или же администратор сервера заблокировал эхозапросы. По сути, команда `ping` и является эхозапросом по протоколу ICMP, на который указанный

в команде адрес должен дать эхоответ — именно его и может заблокировать администратор. Если время отклика удаленных хостов слишком велико и не зависит от месторасположения хостов, то локальный хост подключен к провайдеру с ошибками. Слишком «длинный» путь до удаленного сервера (т.е. большое количество промежуточных маршрутизаторов на пути соединения с сервером) часто приводит к замедлению связи с ним. Если это критично, то имеет смысл попытаться поискать варианты сокращения длины маршрута. Например, в случае игровых серверов можно сделать выбор в пользу тех, которые находятся как можно ближе к серверу провайдера. Если утилиты показывают, что тестовые пакеты не проходят дальше сервера провайдера, то, вероятно, провайдер выполняет плановые профилактические работы.

Очень полезной встроенной утилитой является также команда `ipconfig`, примеры применения которой иллюстрирует таблица 2.

Применение утилит `ping`, `tracert` и `ipconfig` технически не всегда удобно, поскольку для их запуска необходимо открывать окно командной строки и вводить команду с параметрами, которые нужно либо запоминать, либо каждый раз обращаться к справке.

Таблица 2 – Команды утилиты `ipconfig`

№ п/п	Команда	Описание выполнения
1	<code>ipconfig</code>	Отображает краткую информацию о текущей конфигурации протокола IP
2	<code>ipconfig /all</code>	Отображает полную информацию
3	<code>ipconfig /renew</code>	Обновляет сведения для всех адаптеров
4	<code>ipconfig/renew EL'</code>	Обновляет сведения для адаптеров, имя которых

		начинается с букв EL
5	ipconfig/release *EL?1*	Освобождает ip-адреса адаптеров с именами, подходящими под шаблон *EL?1*, Например: EL-1, mELilada

Например, чтобы выяснить путь прохождения пакетов до хоста www.3dnews.ru, требуется в окне командной строки набрать и ввести команду tracert www.3dnews.ru. Результат работы команды, представленный далее, показывает, что хосты разделяют восемь узлов:

C: \Users\naza>tracert www.3dnews.ru

Трассировка маршрута к www.3dnews.ru (195.90.131.231) с максимальным числом прыжков 30:

```

1      <1 ms <1 ms <1 ms vpn237-10.msk.corbina.net
(85.21.0.237)
2      *      *      *      Превышен интервал ожидания для запроса.
3      1 ms  1 ms  1 ms  rti-bb-be4.corbina.net
(195.14.54.149)
4      2 ms  3 ms  3 ms  m9-crs-2-be8.corbina.net
(195.14.62.86)
5      2 ms  2 ms  1 ms  m9-br-be3.corbina.net
(195.14.62.85)
6      35 ms 1 ms  1 ms  Rostelecom-2.corbina.net
(83.102.145.134)
7      2 ms  1 ms  1 ms  188.254.31.98
8      2 ms  2 ms  2 ms  Belyaev.Rosnet.Net
(212.5.174.2)
9      2 ms  2 ms  2 ms  ceta.3dnews.ru
(195.90.131.231)

```

Трассировка завершена.

Применение сетевых утилит позволяет преодолеть неудобство обращения со встроенными утилитами, поскольку обычно они имеют дружественный оконный интерфейс.

Сетевые утилиты — это внешние самостоятельные программные модули и (или) пакеты программ, выполняющие функции специализированных диагностических программных продуктов. Например, программа WinMTR, доступная на сайте, является аналогом консольной утилиты `tracert` и применяется для трассировки маршрута пакета в сети с одновременным определением потерь данных на межсетевых узлах. Программа запускается от имени администратора. Преимуществом утилиты WinMTR являются простота в использовании, отсутствие инсталлятора и возможность выполнения с любого носителя. Для выполнения теста необходимо в поле Host указать имя хоста, например `serfcock.ru`, и нажать кнопку Start. Тест выполняется приблизительно со скоростью 100 пакетов в минуту, что достаточно для получения картины состояния сети.

В колонке Hostname программа выведет IP-адреса маршрутных узлов от хоста-инициатора теста до тестируемого хоста, т. е. будет произведена трассировка маршрута прохождения сигнала. По полученному списку адресов видно, сколько пакетов отправлено (принято) (Sent/Recv), с какими задержками (Best/Avg/Worst/Last) и процентом потерь (Loss%) на каждом из узлов маршрута. Здесь Best/Avg/Worst/Last — соответственно минимальное, среднее, максимальное, последнее время задержки пакета в миллисекундах.

Другой распространенной и доступной на сайте диагностической программой, не требующей установки, является программа `Tcpdump`. Эта программа переводит интерфейс ЭВМ в режим приема всех пакетов, пересылаемых по сетевому сегменту, в котором находится хост — инициатор запуска программы. Программа `Tcpdump` отбирает и отображает на экране пакеты, посылаемые и получаемые хостом. Критерии отбора могут варьироваться, что позволит проанализировать выполнение различных сетевых процедур. В качестве параметров при обращении к программе могут

использоваться наименования протоколов, номера портов и т.д. Например, в результате выполнения команды `tcpdump-q` на консоль по каждому захваченному пакету будет выведена строка, содержащая минимум информации вида `16: 53 : 18.339465 IP ns3.corbina.net.53 > naza-PK.63089 UDP, length 89`

Как видим, строка содержит лишь имя протокола (UDP), сетевые имена, показывающие, откуда (`ns3.corbina.net`) и куда (`naza-PK`) шел пакет, номера портов (53 и 63089) и количество переданных данных (`length 89`). Программа для запуска также требует прав администратора.

Пакет программ Essential NetTools представляет еще один пример сетевой утилиты, которая предназначена для диагностики сети и выявления проблем в ее безопасности. Инструменты программы Essential NetTools могут быть использованы не только для нужд диагностики сетевыми администраторами, но и рядовыми пользователями для наблюдения за любым сетевым соединением. В состав программы входит мощный инструмент PortScan — так называемый сканер портов, который кроме операции «пингования» любого хоста в сети, производит поиск активных TCP-портов в тестируемой сети. Сканер PortScan кроме имени и MAC-адреса хоста показывает все открытые порты, список активных устройств, подключенных в данный момент к сети, а также дополнительную информацию, с помощью которой администратор может определить какие из служб — HTTP, FTP, SMB, iSCSI и (или) SMTP — задействованы на данном хосте. С помощью сканера портов PortScan можно также узнать реальную скорость Интернета. Сохранить все результаты работы по анализу сети PortScan позволяет в удобном формате .xml. Программа работает во всех версиях Windows; она портативная и не требует установки на жесткий диск.

Номенклатура и особенности работы тест-программ

В отличие от программ мониторинга сети, которые выполняет постоянное наблюдение за компьютерной сетью, администраторы сети периодически вынуждены решать повседневные задачи, устраняя относительно несложные, но в то же время наиболее распространенные проблемы локализации дефектов

в объектах сетевой инфраструктуры и оценивая производительность серверов и качество каналов связи. Для этих целей они используют так называемые тест-программы. Номенклатура тест-программы достаточно обширна, о чем свидетельствует далеко не полный список их наименований, приведенный в таблице 3.

Таблица 3 – Номенклатура тест-программы

№ п/п	Имя программы	№ п/п	Имя программы	№ п/п	Имя программы
1	Active Administrator	10	LAN Tornado 1.0	19	Ping
2	AnetTest 1.0-1	11	Local Pinger 1.03		Terminal 2.5
3	CheckHost 1.5 + 3	12	MyVoIPSpeed Server	20	Ping 1.0 build 56
			21	PingMaster 0.9	
4	Connection	13	Network Tools 1.0	22	Port Sweep Demo 2.40
	Checker				
5	Desktop Pinger 1.0	14	NetQuality 3.12	23	Roadkil's ComTest 1.1
		15	Net Runner 1.0		
6	Expert Website Monitor	16	Network Spy 2.0	24	RoboTest 2.0.7
		17	Paessler SNMP Tester	25	TansuTCP 2.1
7	Flexiblesoft Ping 2.0			26	TrafficEmulator
		18	Performance Pinging	27	Winsock Tester 0.0.6
8	Graph-A-Ping 1.0.10				
9	Jac-Ping 1.0				

Широкое распространение тестовых программ объясняется их невысокой стоимостью, удобством в эксплуатации и хорошей эффективностью. В большинстве случаев результаты тестирования сети, будь то определение скорости обмена информацией между компьютером и сетевым ресурсом, локализация участков уязвимости сети и другие, тест-программы выводят не только в цифровом, но и в графическом виде. Как правило, тест-программы применяются для локализации дефектов и «узких мест» в локальных и в распределенных сетях. Типовыми функциями, которые они выполняют,

являются измерение, оценка и контроль производительности работы сетевого оборудования. Рассмотрим назначение наиболее распространенных тест-программ.

Essential NetTools — это мощный пакет, предназначенный для диагностики сети и выявления проблем в ее безопасности.

Инструменты Essential NetTools могут быть использованы не только для нужд диагностики сетевыми администраторами, но новыми пользователями для наблюдения за любым сетевым соединением.

DoSHTTP — это программа проверки Web-серверов на пригодность к эксплуатации в реальной сети. Одновременно DoSHTTP может тестировать несколько серверов. Тестирование производительности программа DoSHTTP выполняет, «забрасывая» Web-сервер потоком пакетов с разными скоростями, и по результатам теста оценивает уровень защиты Web-сервера и его ПО.

PingPlotter — диагностический инструмент для локализации неисправностей в сети. PingPlotter использует комбинацию инструментов, позволяющих выполнять сбор данных в течение заданного интервала времени. Этим интервалом могут быть часы, дни или недели. Выявленные в результате анализа собранных данных потенциальные проблемные участки программа локализует, указывая путь к ним графическими средствами.

Nsauditor Network Security Auditor — это сетевой сканер, служащий для осуществления диагностики и мониторинга сетевых компьютеров на предмет обнаружения возможных проблем в системе безопасности, а также для проверки уровня защиты сети от всех потенциальных уязвимостей, которые хакер может применить для взлома сети.

LanHelper — программа проверки и сканирования офисных и домашних сетей. Программа имеет точный и быстрый сканер, выдающий информацию об IP- и MAC-адресах и позволяющий детально и удобно просматривать данные удаленного компьютера с Web-браузером в режимах просмотра HTML-документов. Кроме того, программа LanHelper позволяет отключать или

перезагружать, а также планировать периодическое и (или) отложенное сканирование удаленных компьютеров.

Особенности работы тест-программ рассмотрим на примере проведения оценочных тестов программой SelfTrend. Свободная версия программы доступна для загрузки на сайте www.prolan.ru/selftrend.

Программа позволяет измерять, оценивать и контролировать производительность работы сетевого оборудования и сетевых сервисов, включая:

- измерение времени реакции файловых сервисов;
- съем SNMP-статистики о работе активного сетевого оборудования;
- получение статистической информации о работе серверов MS Windows;
- получение в режиме реального времени информации о работе сети;
- оповещение о возникающих в сети сбоях посылкой сообщений администратору сети и запуском внешних программ.

Отличительной особенностью программы SelfTrend является реализованный в ней метод пороговых значений, называемый в документации по программе методом светофора. Его суть заключается в следующем. Значения измеряемых характеристик автоматически сравниваются с пороговыми значениями, хранящимися в специальном файле, который называется «модуль знаний». На основании результатов сравнения формируется и выводится на экран интегральная оценка состояния того компонента сети, характеристики которого она измеряет. На экране эта оценка имеет вид светофора. Если значения измеряемых характеристик в норме, то «светофор» горит зеленым светом. Если пороговые значения превышены, то, в зависимости от величины превышения, «светофор» будет выдавать соответствующий сигнал светофора: мигающий желтый, желтый, мигающий красный, красный.

Среди комплекса оценочных тестов программы приведем четыре:

- 1) оценка состояния серверов MS Windows;
- 2) оценка состояния коммутаторов Ethernet;
- 3) интегральная оценка производительности файлового сервиса сети;
- 4) интегральная оценка качества IP-канала в сети VoIP.

Первые три теста ориентированы на тестирование локальных сетей, а четвертый — на тестирование распределенных сетей.

Рассмотрим выполнение первого теста «Оценка состояния серверов MS Windows», который позволяет определить, соответствует ли производительность серверов требованиям используемых в сети приложений. Работа теста основана на автоматическом контроле статистической информации о работе серверов MS Windows NT4/2000/XP. После своего запуска программа SelfTrend предлагает ввести имена серверов, которые должны тестироваться, а также тип ОС MS Windows, которая установлена на этих серверах.

После запуска теста программа подключается к тестируемым серверам и с заданной периодичностью начинает контролировать основные характеристики их работы. Значение каждой характеристики оценивается соответствующим счетчиком. Контролируемые характеристики и диапазоны разрешенных значений соответствующих им счетчиков указаны в таблице 4. В содержательном плане приведенные характеристики означают следующее.

Память (доступно байт) — это объем оперативной памяти на сервере, которая доступна операционной системе в текущий момент времени.

Обмен «память <-> диск» (страниц/с) — это среднее число страниц в секунду, которое ОС сервера была вынуждена прочитать с диска и (или) записать на диск, так как требуемых страниц не оказалось в оперативной памяти сервера в тот момент, когда они потребовались приложению или ОС.

Файл подкачки — если объем этого файла на диске исчерпан, то ОС не сможет запустить новую задачу и будет динамически его расширять, что приведет к резкому падению производительности сервера и «светофор» предупредит, что необходимо увеличить размер файла подкачки.

Процессор (общий процент загрузки процессора) — это процент времени, который приходится на выполнение процессорами сервера полезной работы. Если значение счетчика, отвечающего за эту характеристику, в течение продолжительного времени превышает 85%, то это свидетельствует о недостаточной производительности процессоров сервера. В этом случае следует заменить процессоры более мощными либо переместить часть задач на другие компьютеры.

Таблица 4 – Характеристика оценки серверов

№ п/п	Характеристика	Сигнал «светофора»	
		Зеленый	Красный
1	Память (доступно)	> 64 Мбайт	< 4 Мбайт
2	Обмен «память<->диск» (страниц/с)	< 40	> 120
3	Файл подкачки (общий процент использования)	< 60	> 90
4	Процессор (общий процент загрузки процессора)	< 30	> 85
5	Кэш (процент запросов на получение данных)	> 80	< 20
6	Физический диск (процент активности диска при чтении (записи))	< 5	> 25
7	Физический диск (процент активности диска при чтении (записи))	< 20	> 50
8	Система (время работы системы, с)	> 600	< 600

Кэш (процент запросов на получение данных) — это процент запросов на получение данных, которые уже находятся в оперативной кэш-памяти сервера, поэтому обращение к диску не требуется. Обращения к диску существенно увеличивают время выполнения запросов и, следовательно, снижают производительность работы сервера.

Физический диск (процент активности диска при чтении (записи)) — это процент времени, которое тратится дисковыми устройствами сервера на обработку запросов на чтение (запись) данных. В случае выхода этой

характеристики за пределы, установленные счетчиком, рекомендуется установить на сервере более быстрые диски или переместить активно используемые файлы (например, файлы БД и (или) подкачки) на другие диски.

Система (время работы системы, с) — общее время работы сервера, прошедшее с момента его последней перезагрузки. Считается, что сервер должен перезапускаться как можно реже, поэтому новая перезагрузка (< 10 мин) вызывает мигающий желтый сигнал «светофора».

Диагностика неисправностей средств сетевых коммуникаций

Введение в диагностику кабельных систем

Кабельные системы являются основой построения каналов для передачи и приема информации в сетях. Они всегда проектируются на основе иерархического принципа, благодаря чему получили название «структурированные кабельные системы». Любая перспективная СКС на этапе подготовки к эксплуатации должна быть протестирована специальным оборудованием для выявления тех или иных дефектов и на соответствие заданным характеристикам. От результатов проверки зависит качество и долговечность СКС. Основным практическим интересом при тестировании СКС имеют линии связи на основе витых пар и оптики, чаще других используемые для построения кабельных систем. Для облегчения проектирования и обслуживания СКС на них разработаны стандарты: международный ISO/IEC 11801: 2002-E (далее — международный).

Стандарты призваны обеспечить взаимозаменяемость и универсальное качество СКС наряду с ее доступностью и грамотным использованием. В частности, стандарты телекоммуникационной инфраструктуры зданий должны обеспечить работу разнотипного оборудования любых производителей, создание СКС на этапе строительства зданий и их длительную эксплуатацию.

№ п/п	Частота, МГц	Максимально допустимые значения потерь A _{RL} , дБ			
		Класс C	Класс D	Класс E	Класс F

1	1	15,0/15,0	17,0/19,0	19,0/21,0	19,0/21,0
2	16	15,0/15,0	17,0/19,0	18,0/20,0	18,0/20,0
3	100		10,0/12,0	12,0/14,0	12,0/14,0
4	250			8,0/10,0	8,0/10,0
5	600				8,0/10,0

Таблица 5 – Категории и классы кабельной системы

Категории и классы кабельной системы приведены в таблице 5. Классификации по производительности в международном и американском стандартах отличаются друг от друга.

Международный стандарт определяет классы приложений (от А до F), которые могут работать по данной системе, а американский — специфицирует системы по максимальной частоте передаваемых сигналов (категории 3...7). Поэтому для определения СКС используются как категории, так и классы.

Стандарты определяют среду передачи, параметры разъемов, линии и канала, в том числе предельно допустимые длины, способы подключения проводников, топологию и функциональные элементы СКС.

Реальная кабельная линия всегда имеет неоднородности, которые приводят к отражению электромагнитной волны в процессе прохождения сигнала по кабелю. Обратные потери A_{RL} , дБ, — мера величины отражения сигналов, вызываемого несоответствием импедансом компонентов кабельной системы. Этот параметр определяется как отношение мощности основного сигнала к мощности обратного потока энергии.

Максимально допустимые стандартом ISO-11801 значения потерь A_{RL} , дБ, В формате канал/стационарная линия приведены в таблице 6.

Наиболее распространенной причиной возникновения обратных потерь является различие волнового сопротивления у компонентов кабельного канала (розетка, патчпанель, кабель и т.д.). Поэтому рекомендуется подбирать оборудование одного производителя, обладающее одинаковыми (специально подобранными) характеристиками. Также неоднородность может возникнуть в случае нарушения шага скрутки. Это может быть следствием брака при

производстве либо ошибки монтажников при протяжке кабеля, надлома жилы или слишком сильного изгиба.

Тестирование кабельных систем. Конечные пользователи и проектировщики сетей постоянно планируют более высокие скорости передачи данных, возможности передачи большего количества данных, а также способность сети к гибкой и удобной пере конфигурации.

Таблица 6 – допустимые значения потерь.

№ п/п	Частота, МГц	Максимально допустимые значения потерь A _{RL} , дБ			
		Класс C	Класс D	Класс E	Класс F
1	1	15,0/15,0	17,0/19,0	19,0/21,0	19,0/21,0
2	16	15,0/15,0	17,0/19,0	18,0/20,0	18,0/20,0
3	100		10,0/12,0	12,0/14,0	12,0/14,0
4	250			8,0/10,0	8,0/10,0
5	600				8,0/10,0

До 20% высокоскоростных СКС, как правило, не обеспечивают возможного быстродействия, что является результатом некачественной их реализации. Это особенно хорошо заметно на примерах высокоскоростных систем, в состав которых входят Fast Ethernet, коммутируемые LAN, Gigabit Ethernet.

СКС не существует, пока не проведено ее тестирование. Тестирование СКС определено международным стандартом в трех видах:

1) приемочное тестирование (ПТ) — позволяет принять СКС к эксплуатации, если она сделана в соответствии с рекомендациями стандарта по структуре, топологии и изготовлению и состоит из компонентов с известными характеристиками, отвечающих заранее установленным категориям;

2) тестирование на соответствие (ТС) — позволяет объявить соответствующей стандарту ISO/IEC 11801: 2002(E) кабельную систему, которая содержит не только известные по характеристикам компоненты, но и такие компоненты, характеристики которых заранее неизвестны;

3) эталонное тестирование (ЭТ) — применяется как средство тестирования моделей каналов и линий в лабораторных условиях с помощью лабораторного оборудования, а также как средство для сравнения результатов измерений, полученных с помощью лабораторного оборудования, с результатами, полученными «полевым» измерительным оборудованием. Эталонное тестирование моделей каналов и линий в лабораторных условиях используется также для проверки тех параметров, которые не могут быть протестированы в полевых условиях.

Параметры, измеряющиеся в соответствии с международным стандартом, в таблице 7 отнесены к одной из трех категорий:

- 1) информативные («И») — могут измеряться по согласованию с заказчиком СКС;
- 2) расчетные («Р») — рассчитываются по измеренным параметрам;
- 3) обязательные («О») — измеряются обязательно.

Из таблицы 3 видно, что при приемочном тестировании обязательными параметрами для измерений являются только карта соединений и непрерывность проводников. Однако убедиться в качестве остальных параметров, определяемом именно монтажом, можно только их измерением, поэтому если приемку проводит заказчик, то фактически производится не «приемочное тестирование», а «тестирование на соответствие», даже если соблюдены условия приемочного тестирования.

Таблица 7 – Тестирование параметров измерений

№ п/п	Параметр	Тестирование		
		ПТ	тс	эт
1	Возвратные потери A_{RL}	И	о	о
2	Затухание на ближнем конце NEXT	И	о	о
3	Суммарное переходное затухание на ближнем конце	Р	р	р
4	Защищенность на ближнем конце	И	о	о

5	Суммарная защищенность на ближнем конце	И	р	р
6	Нормированное переходное затухание на дальнем конце	И	о	о
7	Суммарное переходное затухание на дальнем конце	Р	р	р
8	Сопротивление петли по постоянному току	И	о	о
9	Задержка сигнала	Р	о	о
10	Перекося задержки	Р	о	о
11	Длина канала, линии	И	и	о
12	Карта соединений	О	о	о
13	Непрерывность проводников, экранов, КЗ и обрывы	О	о	о

Основным инструментом для оперативного тестирования кабельных систем, реализованных на основе витых пар, являются кабельные сканеры.

Одна из наиболее удобных и важных функций тестирования кабельных систем — автоматизация процесса проведения измерений и интерпретация полученных результатов. Во время общего теста (режим Autotest) в течение нескольких секунд последовательно, без вмешательства оператора, измеряется ряд необходимых для проверки параметров. Результаты измерений сравниваются с требованиями стандартов, после чего выдается заключение в виде: «выполняется/не выполняется». Время автотеста составляет около 10...20 с. Многие сканеры поддерживают голосовую связь во время тестирования, что очень удобно при тестировании распределенной СКС.

Практические рекомендации по тестированию СКС. Правила использования полевых тестеров определены их подробными инструкциями, которая должна быть изучена досконально. Однако приведенные далее рекомендации следует учитывать при пользовании любым из этих приборов.

1. При проведении тестирования необходимо представлять, по каким критериям проводится тестирование. Как правило, полевые тестеры имеют режим «Автотест», в котором могут использоваться американский,

международный или другие стандарты, поэтому необходимо однозначно выбрать стандарт и набор параметров, подлежащих измерению.

2. Необходимо точно знать скорость распространения сигнала в том кабеле, из которого сделана линия, и на котором проводятся измерения. Для кабелей скорость распространения сигнала обязательно указывается в спецификации, а полевые тестеры, как правило, хранят библиотеку этих значений для конкретных типов изделий. Скорость распространения сигнала по кабелю принято характеризовать параметром NVP, который указывается в долях от скорости света. В четырех парных кабелях значения NVP находятся в пределах от 0,6 до 0,8. Тестеры обычно имеют функцию калибровки NVP, которая позволяет на образце данного кабеля известной длины определить этот параметр. Минимальная длина кабеля при этом должна быть более 15 м; чем она больше, тем лучше, поскольку точность в значении NVP будет определять точность измерения длины полевым тестером.

3. Необходимо прокалибровать прибор именно при выбранных критериях перед началом измерений.

4. Тестовые шнуры и измерительные адаптеры изнашиваются в процессе эксплуатации и погрешности прибора возрастают. Поэтому стандарт IEC 61935-1 настоятельно рекомендует владельцу тестера создать «эталонную» линию и периодически проверять по ней свой прибор.

Особенности проверки электрической подсистемы СКС. Тестирование электрической подсистемы СКС выполняется с помощью рефлектометра, принцип действия которого основан на анализе сигнала, отраженного от различных неоднородностей в линии при ее зондировании мощными импульсами тока небольшой длительности.

Электрическая волна, возбуждаемая в тестируемой линии импульсным генератором рефлектометра, при распространении в линии отражается в обратном направлении от всех точек неоднородностей. Анализатор приемника контролирует как момент прихода отраженного сигнала, так и изменение его формы во времени. Результат работы анализатора может быть представлен на

дисплее графически, в виде так называемой рефлектограммы, или же в табличной форме. По времени задержки между зондирующим и приходящим импульсом рассчитывается расстояние до неоднородности, и его значения выводятся на экран.

Рефлектограммы для электрических кабелей получили широкое распространение в сетях городской и междугородной связи. Из-за трудностей анализа начального участка они эффективны только в процессе тестирования кабелей магистральных подсистем и поэтому не получили широкого распространения в технике СКС. При тестировании кабельных систем здания их роль успешно выполняют кабельные сканеры, реализующие функции рефлектометра.

Особенности тестирования оптоволоконных сетей. Процедуры тестирования оптоволоконных линий и каналов СКС, построенных в соответствии с международным стандартом, определены международным техническим документом ISO/IEC TR 14763-3, в котором указаны следующие характеристики СКС, подлежащие проверке:

- целостность оптоволокон;
- длина линий и каналов;
- задержка оптических сигналов;
- ослабление оптических сигналов.

Целостность оптоволокон разрешается определять любым прибором, начиная от любого простого источника света и заканчивая оптическими рефлектометрами. В СКС, где длины внутри объектовых кабелей не превышают 100 м, для этой цели удобно использовать недорогие (250 долл. США) определители обрывов.

Длина линий и каналов определяется по длине кабелей СКС или рефлектометром.

Задержка оптических сигналов определяется расчетным путем по известным значениям длины линий и группового показателя преломления

оптоволокна, обычно указываемого производителем кабеля. Как правило, задержка сигналов в оптоволокне составляет 5 нс/м.

Ослабление оптических сигналов при наладочных измерениях можно измерять относительно недорогими оптическими тестерами, содержащими источник света и измеритель мощности. При ответственных измерениях, имеющих целью установить соответствие установленной СКС международному стандарту, необходимо применять качественные приборы, отличающиеся от простых оптических тестеров гарантированной спектральной шириной источника излучения, стабильностью и точностью прибора.

Оборудование для проверки кабельных систем

Оборудование для проверки кабельных систем. Оно подразделяется на четыре группы: сетевые анализаторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры. При этом для каждого вида проверок, приведенных в таблице 8, необходимо применять только соответствующее этому виду оборудование.

Сетевые анализаторы — это эталонные измерительные инструменты для диагностики и сертификации кабелей и СКС. Примером сетевого анализатора может служить устройство HP 85 компании Hewlett-Packard.

Сетевые анализаторы являются интеллектуальными устройствами, способными работать на физическом, канальном, а иногда и на сетевом уровнях. В их состав входят высокоточный частотный широкополосный генератор и узкополосный приемник, позволяющие измерять на приемной паре амплитудно-частотную характеристику, перекрестные наводки, затухание, суммарное затухание, параметр NEXT.

Кроме того, с их помощью можно измерять среднюю интенсивность общего трафика сети и среднюю интенсивность потока пакетов с определенным типом ошибки. Сетевой анализатор представляет собой лабораторный прибор больших размеров, достаточно сложный в обращении, стоимостью более 20 000 долл. США.

Далее рассмотрены портативные диагностические устройства, доступные практически каждому администратору ЛВС.

Таблица 8 – Виды операций тестирования

№ п/п	Вид контрольной операции	Оборудование
1	Эталонное тестирование кабелей разных категорий	Сетевой анализатор
2	Проверка кабеля на отсутствие физического обрыва	Тестеры
3	Диагностика медных кабельных систем	Кабельные сканеры
4	Сертификация СКС на соответствие определенному стандарту. Диагностика СКС	Портативные устройства для сертификации СКС

Кабельные сканеры используются для диагностики медных кабельных систем. Основное назначение кабельных сканеров — измерение электрических и механических параметров кабелей: длины кабеля, параметра NEXT, затухания, импеданса, схемы разводки пар проводников, уровня электрических шумов в кабеле. Точность измерений, произведенных этими устройствами, ниже, чем у сетевых анализаторов, но вполне достаточная для оценки соответствия кабеля стандарту.

Для определения местоположения неисправности кабельной системы (обрыва, короткого замыкания, неправильно установленного разъема и т.д.) используется метод отраженного импульса. Суть этого метода заключается в том, что сканер излучает в кабель короткий электрический импульс и измеряет время задержки до прихода отраженного сигнала. По полярности отраженного импульса определяется характер повреждения кабеля (короткое замыкание или обрыв). В правильно установленном и подключенном кабеле отраженный импульс почти отсутствует.



(a)



(б)

Рисунок 4 – Кабельный сканер PentaScanner (a) и кабельный тестер (б)

Точность измерения расстояния зависит от того, насколько точно известна скорость распространения электромагнитных волн в кабеле, которая задается в процентах от скорости света в вакууме. Современные сканеры содержат в себе электронную таблицу данных об этом параметре для всех основных типов кабелей, что дает возможность пользователю после калибровки сканера устанавливать их самостоятельно. На рисунке 4, а представлен современный многофункциональный сканер семейства моделей PentaScanner компании Microtest, который применяется для сертификации кабельных систем категории 5. Он предназначен для поиска неисправностей кабельной системы и представляет собой недорогой и простой в использовании прибор, позволяющий быстро определить неисправность кабельной системы. Кабельный сканер PentaScanner содержит несколько частотных генераторов и узко-полосных приемников, графический дисплей на жидких кристаллах и флэш-память для записи результатов тестирования и новых версий ПО. Как элемент питания PentaScanner использует аккумуляторные батареи, работающие без подзарядки до 10 ч. Прибор содержит разъемы для прямого присоединения к кабелю.

Для измерения перекрестных наводок между витыми парами (NEXT) источник сигналов — Super Injector (прибор, поставляемый в комплекте с PentaScanner) — подсоединяется к передающей паре и начинает передавать в нее сигналы различной частоты. Приемник сигналов подключается к приемной паре и измеряет сигнал, наведенный в ней, сравнивая его со стандартными величинами. Преимуществом узкополосного приемника в PentaScanner является

измерение чистого NEXT с отфильтровыванием всех наводок и электрического шума. Для измерения затухания PentaScanner использует Super Injector+ в качестве удаленного источника сигналов, генерирующего серию сигналов различной частоты. Сканер PentaScanner в этот момент измеряет амплитуду этих сигналов на другом конце кабеля.

Кабельный тестер, показанный на рисунке 3.6.2.1, б, — это наиболее простой и дешевый прибор для диагностики витой пары. Он позволяет определить непрерывность кабеля, не указывая места сбоя. Кабельный тестер этого типа показывает только минимальное соответствие характеристик канала связи заложенным в него требованиям. Этот тип кабельного тестера служит для повышения эффективности монтажа проводки и оперативного обнаружения неисправностей.

Оборудование для проверки оптоволоконных СКС. Оно очень разнообразно. Рассмотрим назначение отдельных его представителей.

Измеритель оптической мощности используется для измерения оптической мощности сигнала и в паре со стабилизированным оптическим излучателем применяется для измерения затухания в кабеле. Основным показателем качества измерителя является тип примененного в нем фотодиода. Наилучшие характеристики имеет фотодиод на основе арсенида галлия.

Анализатор затухания — это комбинация оптического измерителя мощности и источника оптического сигнала. Выпускается он в виде набора из измерителя, излучателей на разных длинах волн и комплекта оптических интерфейсов, показанных на рисунке 5.



Рисунок 5 – Комплект оптических интерфейсов

Оптические аттенюаторы используются для моделирования потерь в оптической линии при стрессовом тестировании сети, при измерении коэффициента ошибок, калибровке и проверке измерителей мощности, тестировании оптоэлектронных и электрооптических преобразователей, анализе допустимых потерь оптического сигнала на всем пути от передатчика до приемника (эти потери называются оптическим бюджетом линии).

В оптических аттенюаторах используются различные методы внесения затухания: осевое и радиальное смещение, использование фильтров и призм. Для согласования излучающего и приемного торцов световодов применяются согласующие узлы, фокусирующие излучение.

Основными характеристиками оптических аттенюаторов являются: точность, линейность, уровень возвратных потерь, повторяемость установления затухания, разрешение, остаточное вносимое затухание.

Оптические рефлектометры являются наиболее информативными и мощными средствами тестирования волоконно-оптических линий.

На рисунке 6 показан оптический рефлектометр OptiFiber Pro, позволяющий обнаруживать, идентифицировать и измерять эффекты отражения и потерь в многомодовых и одномодовых волоконно-оптических линиях. Номинальная предельная дальность измерений составляет 35 км при длине волны 1 300 нм в многомодовых оптических линиях и 130 км при длине волны 1 550 нм в одномодовых оптических линиях.

Большинство рефлектометров имеет встроенное ПО для автоматического определения и анализа участков аномального затухания и разрывов. Все, что требуется от специалиста, — это подключить устройство к кабельной линии и нажать кнопку, а затем ознакомиться с результатами измерений. Благодаря применению рефлектометра можно быстро находить дефекты на линии связи и иметь представление об их характере, чтобы заранее знать, какие меры предпринять для их устранения. Современные рефлектометры имеют очень

высокий уровень точности. Оптические рефлектометры имеют следующие особенности:

- за один цикл они позволяют измерять целый ряд параметров (длину, затухание и местонахождение неоднородности);
- допускают выполнение измерений с одного конца кабеля;
- высокие требования к качеству ввода излучения в тестируемое волокно;
- достаточно малое время получения рефлектограммы — около 30с.

Оптический локатор — это упрощенный вариант рефлектометра. Принцип его действия идентичен работе рефлектометра, а упрощение достигнуто за счет отказа от графического дисплея и применения более простого ПО. Функция «визуализатор дефектов» является одной из наиболее полезных функций оптического локатора. Визуализатор дефектов предназначен для выявления близких к концу кабеля (не более 5 км) обрывов и других дефектов, волоконных световодов методом просветки. Основой прибора является лазер красного свечения. При подключении визуализатора к волокну в месте повреждения наблюдается красное свечение.

Идентификаторы кабеля применяют для неразрушающего тестирования его целостности, проверки маркировки кабеля, подтверждения наличия или отсутствия сигнала в линии, определения вида модуляции, а также для ввода-вывода оптического сигнала через изгиб кабеля.



Рисунок 6 – Оптофоны

Последняя возможность эффективно используется для организации связи по проложенному кабелю, когда идентификаторы кабеля используются в комплекте с оптическими разговорными устройствами. Идентификаторы удобны для пошагового прохода (трассировки) оптического кабеля.

Анализатор возвратных потерь измеряет суммарный уровень отражения во всей линии, включая кабель, оптические интерфейсы и разветвители. Возвратные потери приводят к понижению отношения сигнал/шум в аналоговых системах и увеличению параметра ошибки в цифровых системах передачи. В качестве источника сигнала обычно используется лазерный диод в режиме и непрерывного излучения, а в качестве измерителя мощности отраженного сигнала — измерители оптической мощности. Очень важна стабильность источника сигнала, поскольку спектральная нестабильность источника приводит к удвоению ошибки измерения за счет отражения.

Оптические разговорные устройства (оптофоны), представленные на рисунке 3.6.2.3, обеспечивают голосовую связь по оптическому кабелю при его прокладке и тестируют его работоспособность. Голосовая оптическая связь обеспечивает взаимодействие между бригадами, производящими укладку кабеля. В полудуплексных оптофонах режим передачи переключается вручную или активируется голосом. В полнодуплексных оптофонах прием и передача осуществляются одновременно на двух разных длинах волн или применяется временное разделение сигналов на одной длине волны.

Динамический диапазон современных оптофонов достигает 60 дБ, что позволяет разговаривать на расстоянии до 150 км.

Лабораторная работа

Тема: Диагностика работы компьютерной сети

Цель работы: Проанализировать особенностей работы тест - программ. Выполнить мониторинг сети с использованием программы – анализатора протоколов Wireshark и сканера сети LanHelper.

Порядок выполнения работ

1. Проанализировать особенностей работы тест – программ таблица 1.3 – Номенклатура тест-программы
2. Выполните мониторинг компьютерной сети программой Wireshark. Запустите программу в режиме захвата трафика, проходящего через интерфейс, подключенный к локальной сети (обычно это eth0). На рисунке 1.1 показано главное окно программы. Перейдите к следующему заданию.

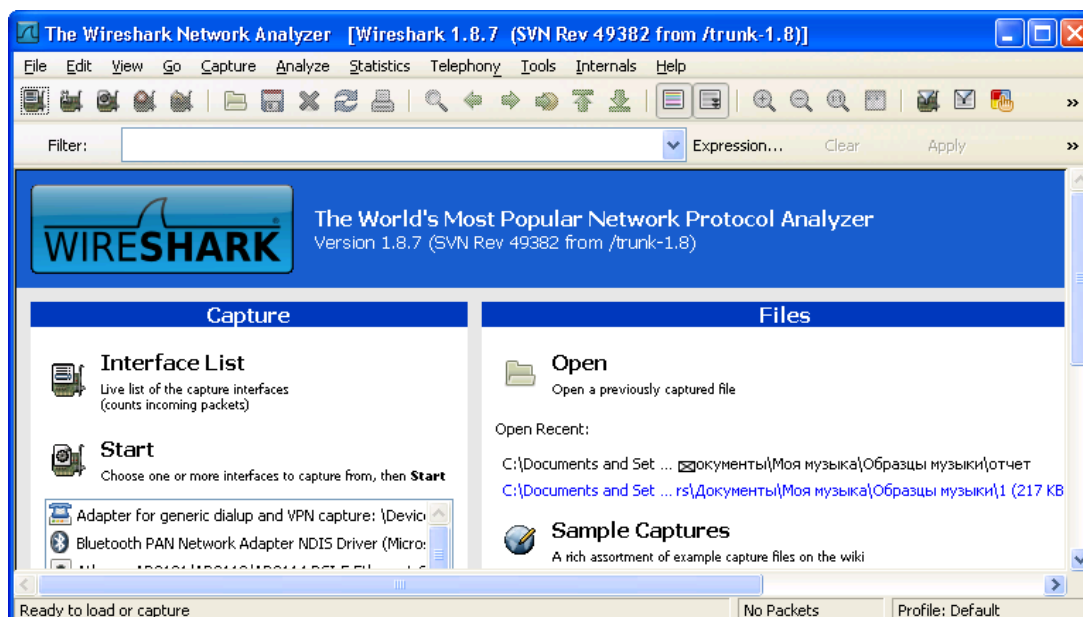


Рисунок 1.1 – Главное окно программы

3. Эмулируйте сетевую активность в течении 10-15 минут. Для этого можно выполнить, например, некоторые из указанных действий (на выбор). На рисунке 1.2 показан запуск программы.
- Откройте сайт <http://rtos.asoiu>;
 - Подключитесь к серверу <ftp://telecom.asoiu>;
 - Выполните пинг любых узлов;
 - Подключитесь к одному из доступных сетевых дисков Windows (если такие ресурсы представлены в сети)
 - Откройте сайт <http://telecom.asoiu>;
 - Выполните прочие действия, требующие сетевого подключения.

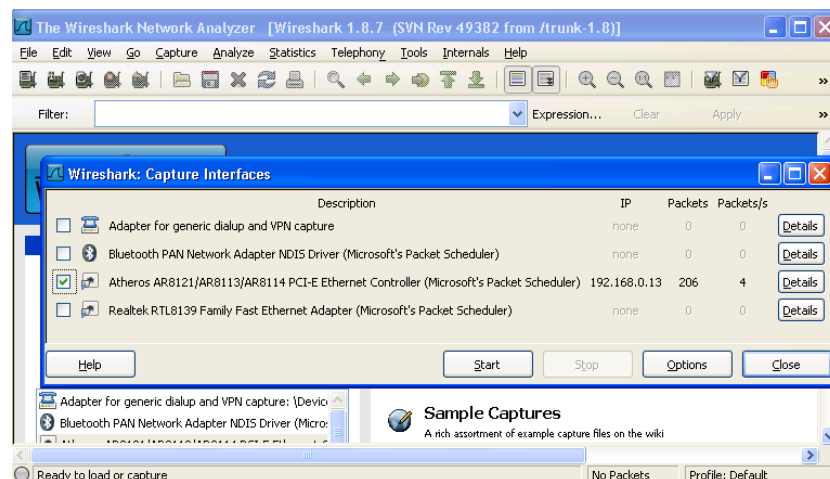


Рисунок 1.2 – Запуск сканирования

В соответствии с рисунком 1.3 останавливаем захват.

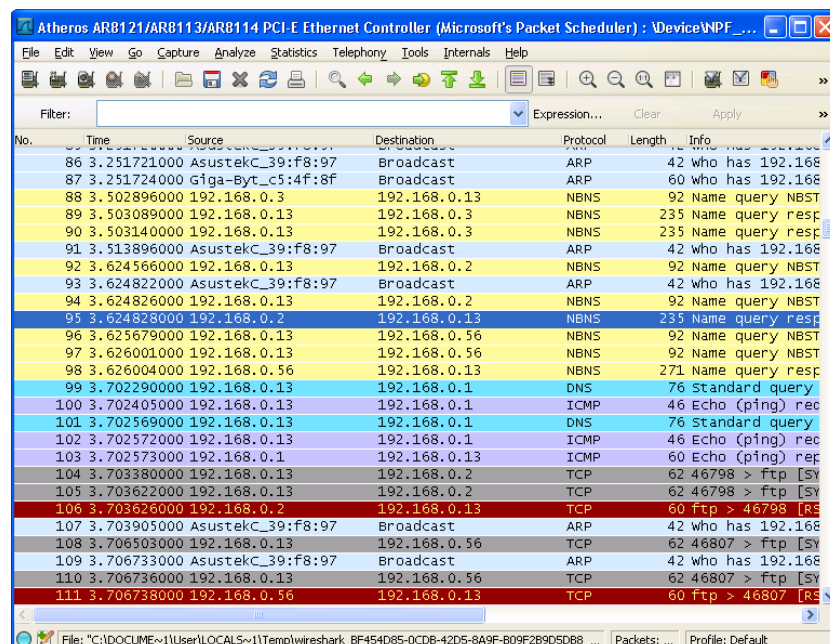


Рисунок 1.3 – Останавливаем захват

На рисунке 1.4 показан суммарный захват

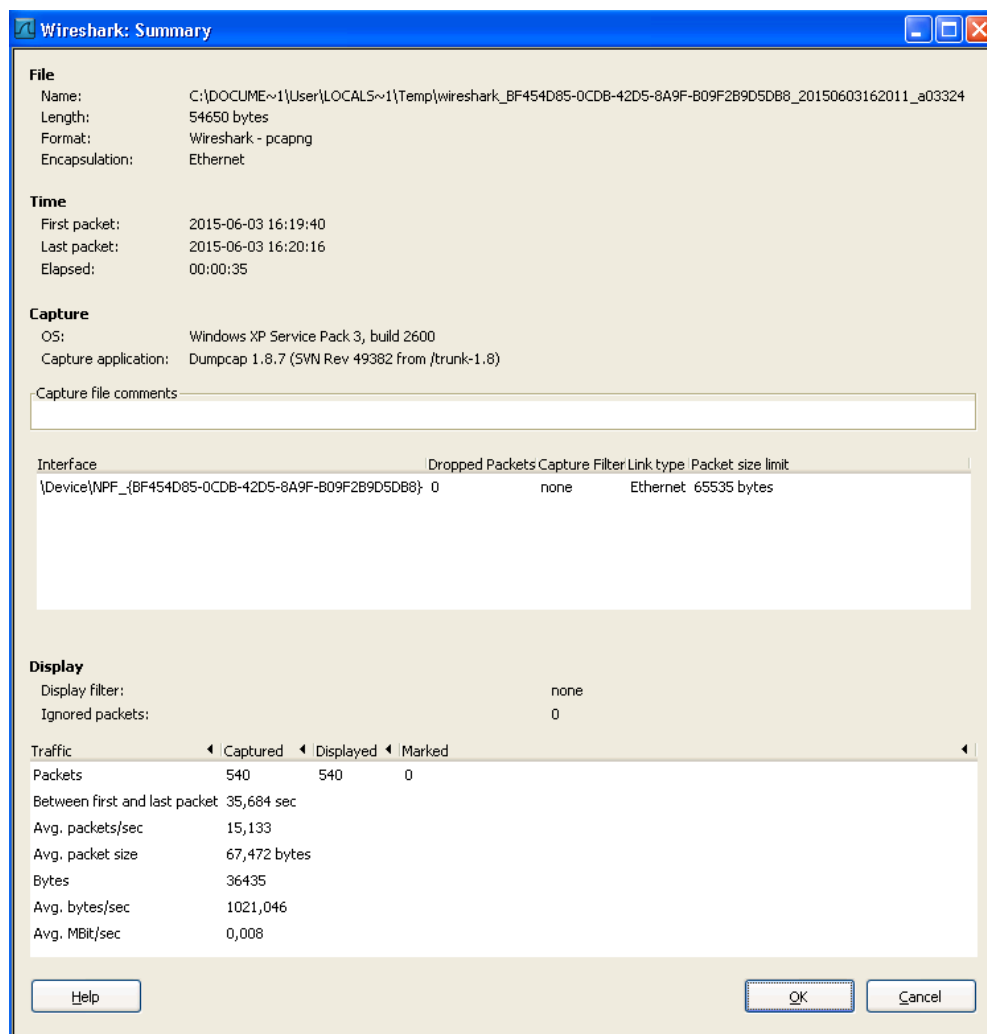


Рисунок 1.4 – Захват

4. Заполните таблицу 1.1. Исходные данные для таблицы представлены в отчете Statistics/Summary. При заполнении таблицы обратите внимание на соблюдение размерности величин (кб, Мб, Мбит).

Таблица 1.1 – Учёт трафика

Параметр	Значение
Время захвата, сек	
К-во захваченных пакетов	
Объем, Мб	
Средн. размер пакета, Кб	
Средняя скорость, пакетов/сек	
Средняя скорость, Мбит/сек	

5. Составить таблицу 1.2 распределения трафика по протоколам. На рисунке 1.5 показаны данные по протоколам. Исходные данные для таблицы можно получить из отчета Statistics/ Protocol Hierarchy.

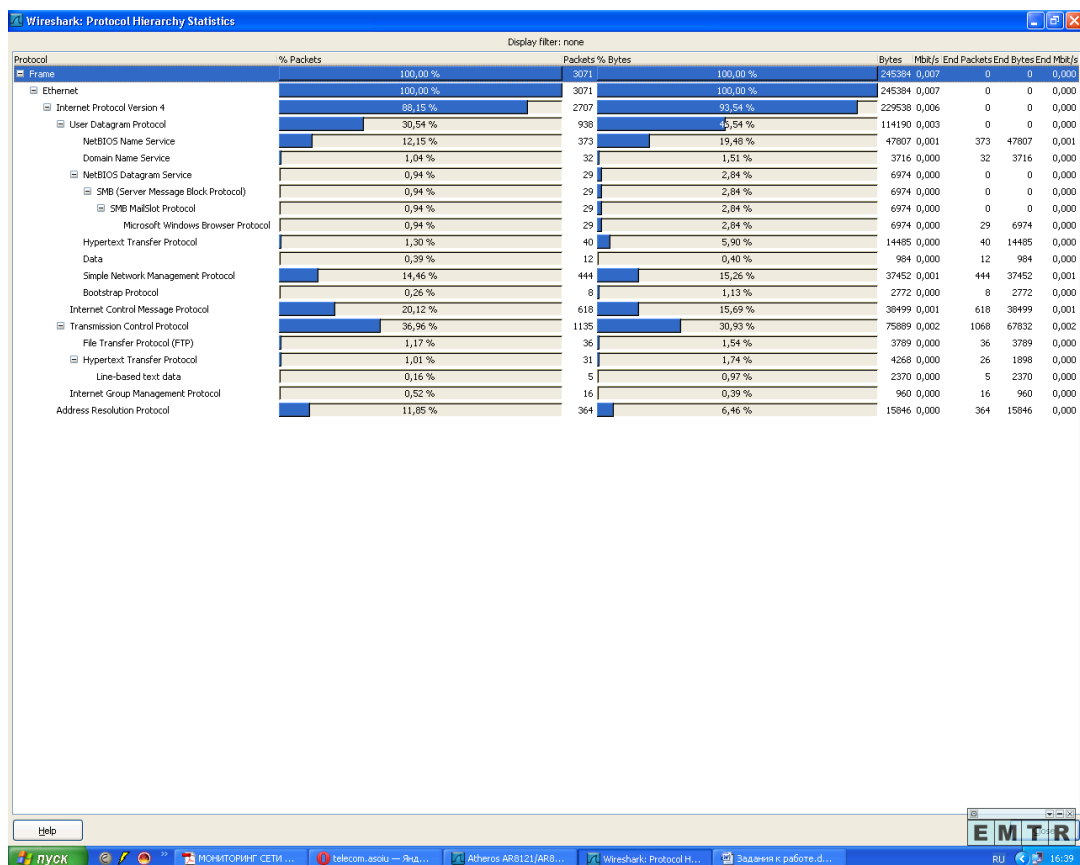


Рисунок 1.5 – Распределение трафика по протоколам

Таблица 1.2 – Распределение трафика по протоколам

Протокол	Трафик, мб	Трафик, %
Frame		
ethernet		
IPv4		
UDP		
NetBIOS Name Servise		
DNS		
NetBIOS Datagram Servise		
SMB(seres message block protocol)		
SMB MailSlot Protocol		
Microsoft Windows Browser Protocol		
Hypertext Transfer Protocol		
Data		
Simple Network Management Protocol		
Bootstrap Protocol		
Internet Control Message Protokol		
Transmission Control Protocol		
File Transfer Protocol (FTP)		
Hypertext Transfer Protocol		
Line-based text data		
Internet Group Management Protocol		
Address Resolution Protocol		
Итого		

6. Составить таблицу 1.3 распределения Ethernet-трафика по узлам сети. Исходные данные для заполнения таблицы получить из отчета Statistics/Endpoint list/Ethernet указаны на рисунке 1.6. На рисунке 1.7 показан отчет.

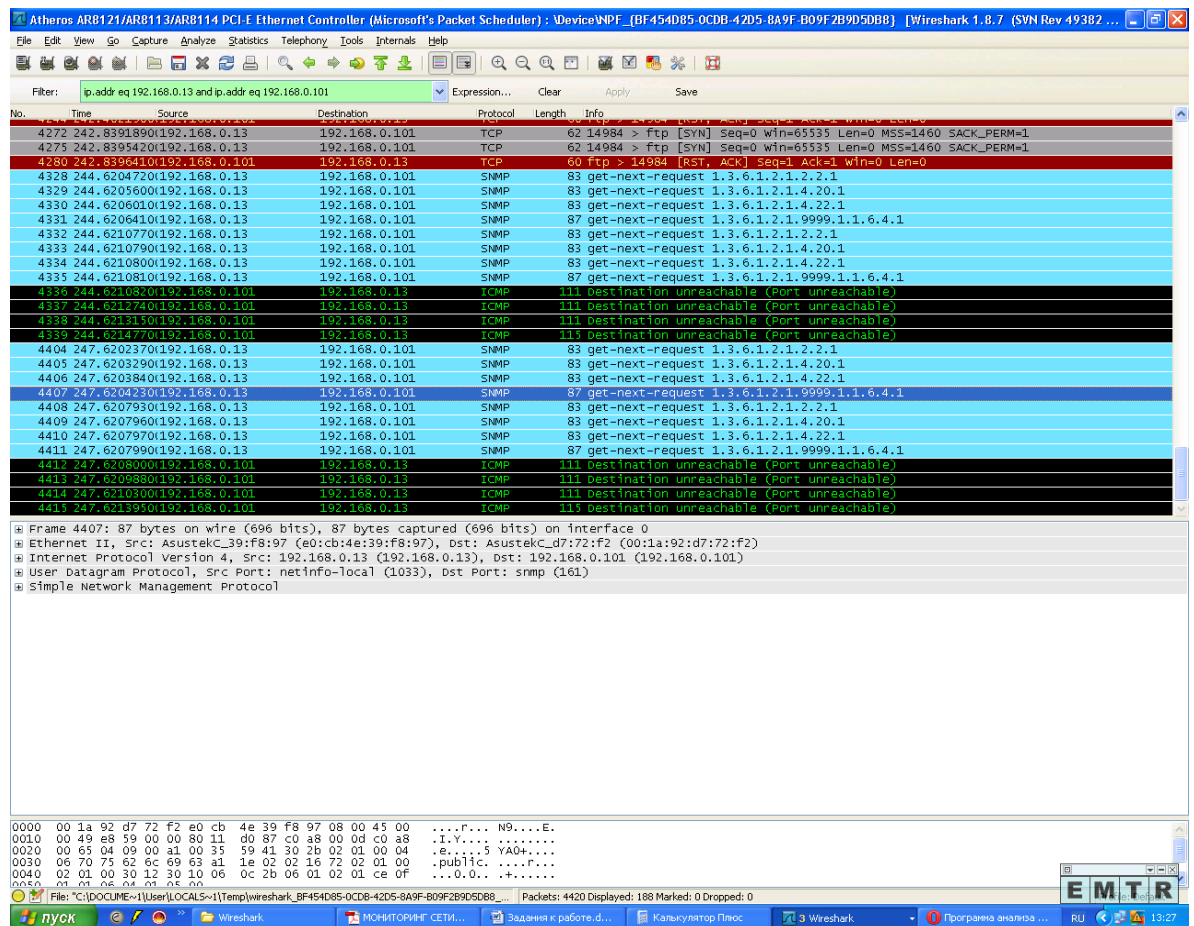


Рисунок 1.6 – Статистика

Endpoints: Atheros ARB121/ARB113/ARB114 PCI-E Ethernet Controller (Microsoft's Packet Scheduler) : \Device\NPF_{BF454D85-0CDB-42D5-8A9F-B09F2B9D5DB8}									
Ethernet: 20 Fibre Channel: FDDI: IPv4: 24 IPv6: IPX: JXTA: NCP: RSVP: SCTP: TCP: 287 Token Ring: UDP: 234 USB: WLAN:									
IPv4 Endpoints									
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude	
192.168.0.1	454	39 883	192	19 039	262	20 844	-	-	-
192.168.0.13	3 750	314 074	2 583	193 097	1 167	120 977	-	-	-
192.168.0.3	529	43 714	257	20 882	272	22 832	-	-	-
192.168.0.255	37	5 221	0	0	37	5 221	-	-	-
192.168.0.105	171	13 551	56	5 437	115	8 114	-	-	-
192.168.0.11	206	16 491	18	2 655	188	13 836	-	-	-
192.168.0.106	264	21 181	92	8 555	172	12 626	-	-	-
192.168.0.104	272	21 653	84	9 371	188	12 282	-	-	-
192.168.0.101	219	18 134	75	7 304	144	10 830	-	-	-
192.168.0.56	237	19 351	73	7 221	164	12 130	-	-	-
192.168.0.107	195	16 483	59	6 057	136	10 426	-	-	-
192.168.0.109	337	30 377	99	13 893	238	16 484	-	-	-
192.168.0.6	91	8 418	19	2 898	72	5 520	-	-	-
192.168.0.103	226	18 414	74	7 210	152	11 204	-	-	-
192.168.0.230	90	8 499	18	2 979	72	5 520	-	-	-
192.168.0.7	63	4 404	9	540	54	3 864	-	-	-
192.168.0.5	91	8 418	19	2 898	72	5 520	-	-	-
192.168.0.108	161	12 498	51	4 968	110	7 530	-	-	-
92.51.156.76	3	222	3	222	0	0	-	-	-
192.168.0.2	223	17 954	70	6 747	153	11 207	-	-	-
192.168.0.102	206	17 377	64	6 579	142	10 798	-	-	-
255.255.255.255	8	1 190	0	0	8	1 190	-	-	-
178.35.137.123	2	169	2	169	0	0	-	-	-
77.234.43.63	1	234	1	234	0	0	-	-	-

Рисунок 1.7 – Отчет

Таблица 1.3 – Распределение трафика по узлам сети

IP- адрес	Трафик					
	входящий		исходящий		общий	
	Мб	%	Мб	%	Мб	%
192.168.0.1						
192.168.0.13						
192.168.0.3						
192.168.0.255						
192.168.0.105						
192.168.0.11						
192.168.0.106						
192.168.0.104						
192.168.0.101						
192.168.0.56						
192.168.0.107						
192.168.0.109						
192.168.0.6						
192.168.0.103						
192.168.0.230						
192.168.0.7						
192.168.0.5						
192.168.0.108						
92.51.156.76						
192.168.0.2						
192.168.0.102						
255.255.255.255						
178.35.137.123						
77.234.43.63						
Итого:						

7. По данным таблицы 1.1 определить относительную загрузку сети (в %) за контрольный период времени по формуле:

$$\text{Загрузка} = \frac{(\text{Трафик, Мбит/Время, сек}) * 100}{\text{Пропускная способность, Мбит/сек}}$$

8. По данным таблицы 1.2 сделайте выводы о качественном составе трафика, т.е. о соотношении прикладных и служебных протоколов.

Самый загруженный по протоколам является ТСР/ІР.

9. По данным таблицы 1.3 определите, какие из узлов являются наиболее загруженными с учетом направления трафика (исходящий, входящий, общий).

10. Скачайте и установите любую из программ таблицы № 5. Выполните ей диагностику работы сети

11. Оформите отчет по выполненной работе

Контрольные вопросы

1. Дайте определение понятий «диагностика» и «тестирование сети».
2. Изложите основные принципы локализации неисправностей сети.
3. Как связана модель OSI с локализацией неисправностей сети?
4. Для чего необходимо документирование сети?
5. Для каких целей проводится входное и нагрузочное тестирование сети?
6. В чем состоит принцип нагрузочного тестирования?
7. В чем состоит принцип выбора правильного инструмента диагностики?
8. В чем состоит принцип декомпозиции сетевой проблемы?
- Э. В чем состоит принцип локализации неисправностей «сверху вниз»?
10. Проведите классификацию сетевых проблем по уровням модели OSI.
11. Изложите принципы локализации дефектов при проведении нагрузочного тестирования.
12. Изложите методику проведения нагрузочного тестирования сети.
13. Какие типы нагрузочных тестов вам известны?
14. Что проверяет тест FTest all stations с нагрузкой только на сеть?
15. Поясните зависимости параметров функционирования Агентов от величины предлагаемой нагрузки на сеть Ethernet.
16. Расскажите о встроенных в ОС средствах диагностики сети.
17. Дайте определение сетевых утилит.
18. Расскажите о назначении и интерфейсе сетевых утилит WinMTR и Tcpdump.
19. Расскажите о назначении и интерфейсе программы Essential NetTools.

20. Расскажите о функциях сетевых тест-программ.
21. В чем состоят особенности работы тест-программы SelfTrend?
22. Какие категории и классы кабельной системы вам известны?
23. Расскажите о порядке тестирования каналов и стационарных линий СКС.
24. Назовите параметры тестирования линий кабельных систем.
25. Изложите правила тестирования кабельных систем.
26. Расскажите об оборудовании для проверки оптоволоконных СКС.

Контрольный тест

1. Как называется процедура сбора первичных данных о работе сети: статистики о количестве циркулирующих в сети кадров и пакетов различных протоколов, состоянии портов концентраторов, коммутаторов и маршрутизаторов?

- а) мониторинг;
- б) анализ;
- в) диагностика;
- г) тестирование.

2. Как называются средства, представляющие собой программные или аппаратно-программные системы, которые выполняют функции мониторинга и анализа трафика в сетях, собирающие данные о работе протоколов всех уровней сети?

- а) экспертные системы;
- б) встроенные системы диагностики и управления;
- в) анализаторы протоколов;
- г) агенты систем управления.

3. Как называются средства, аккумулирующие знания технических специалистов о выявлении причин аномальной работы сетей и возможных способах их устранения?

- а) multifunctional портативные устройства анализа и диагностики;

- б) экспертные системы;
- в) встроенные системы диагностики и управления;
- г) анализаторы протоколов.

4. Как называется измерение характеристик работы сети в процессе ее эксплуатации (без остановки работы пользователей)?

- а) диагностика сети;
- б) мониторинг работы сети;
- в) анализ работы сети;
- г) тестирование сети.

5. Назовите для чего не проводится нагрузочное тестирование?

- а) для маркировки компонентов ЛВС;
- б) для получения интегральной оценки качества работы модифицируемой (новой) сети и определения запаса ее производительности;
- в) выявления скрытых дефектов сетевых адаптеров и драйверов;
- г) измерения производительности и выявления скрытых дефектов активного сетевого оборудования;
- д) сравнения эффективности различных сетевых архитектур;
- е) (для проведения аудита основных и резервных источников питания).

6. Как называется утилита, которая отображает статистику протокола и текущих сетевых подключений tcp/ip?

7. Как называется утилита, которая проверяет наличие связи с указанным узлом?

8. Как называется утилита, которая выводит имена и IP-адреса всех маршрутизаторов, через которые проходят пакеты от локального компьютера к указанному узлу?

СПИСОК ЛИТЕРАТУРЫ

А.В. Назарова Эксплуатация объектов сетевой инфраструктуры [Текст] / А.В. Назарова Москва: «Академия», 2014. – 166 с.

Зорина Л.Я. Дидактические аспекты естественно научного образования [Текст] / Зорина Л.Я. Москва: РАО, 1993.- 163 с.

Олимов К.Т. Проблемы создания учебников специальных дисциплин нового поколения в сфере среднего специального и профессионального образования [Текст] / Олимов К.Т. Ташкент: «Фан».-2004 - 143с.

Уилсон Эд Мониторинг и анализ сетей Методы выявления неисправностей [Текст] / Уилсон Эд. – Издательство "ЛОРИ", 2002. – 163 с.

Андреев А.А. Дидактические основы дистанционного обучения в высших учебных заведениях [Текст] / Андреев А.А.: МЭСИ. 2004. -48с

Логинов М. Д. Техническое обслуживание средств вычислительной техники: учебное пособие [Текст] / М. Д. Логинов, Т. А. Логинова. — М. : БИНОМ. Лаборатория знаний, 2010. — 182 с.

Хожиев А. Х. Особенности, преимущества и эффективность электронных учебников по специальным дисциплинам, применяемых в профессиональных колледжах [Текст] / Хожиев А. Х. Молодой ученый. — 2012. — №2. — С. 311-313.

Поляк-Брагинский А. В. Локальные сети. Модернизация и поиск неисправностей [Текст] / Поляк-Брагинский А. В 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2009. — 462 с.

Гребешков А.Ю. Управление сетями электросвязи по стандарту TMN [Текст] / Гребешков А.Ю. Учеб. пособие.- М.: Радио и связь, 2004 г. – 132с

Закер Крейт Компьютерные сети модернизация и поиск неисправностей [Текст] / Закер Крейт - Перевод на русский язык «ВХВ-Петербург». 2001. — 368 с:

Бигелоу С. Сети: поиск неисправностей, поддержка и восстановление [Текст] / Бигелоу С.:Пер. с англ. – СПб.: БХВ-Петербург, 2005. – 642с

Колисниченко Д. Н. Сделай сам компьютерную сеть. Монтаж, настройка, обслуживание [Текст] / Колисниченко Д. Н. — СПб.: Наука и Техника, 2004. — 155 с.

Архипова, О.Б. Администрирование информационных систем (в операционных системах Windows) [Текст] / О.Б. Архипова, Т.М. Медведская. — Новосибирск: СГГА, 2011. — 83 с.

Ретинская И.В., М.В.Шугрина «IBM и Makintosh в сфере образования». [Текст] / Ретинская И.В., М.В.Шугрина Мир, ПК - № 3. 1994.

Беляев М.И., Вымятнин В.М., Григорьев С.Г. Теоретические основы создания образовательных электронных изданий [Текст] / Беляев М.И., Вымятнин В.М., Григорьев С.Г. Томск: Том. Ун-та, 2002. — 86 с.

Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов [Текст] / Олифер В.Г., Олифер Н.А. 4-е издание СПб: Питер, 2010 — 56 с.

Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. / В.Г. Олифер, Н.А. Олифер 2-е издание СПб: Питер, 2001 — 123 с.

ГОСТ 21.101-97. Основные требования к проектной и рабочей документации.

ГОСТ 2.105-95. Единая система конструкторской документации. Общие требования к текстовым документам. Межгосударственный совет по стандартизации, метрологии и сертификации. - Минск. 2000.

ГОСТ 21.110-95. Правила выполнения спецификации оборудования, изделий и материалов. Система проектной документации для строительства. — М., 1995.-12 с

ГОСТ Р 50739. Защита от несанкционированного доступа к информации. Общие технические требования. - 10 с.

IBM DeveloperWorks [Электронный ресурс] — Режим доступа: <http://www.ibm.com/developerworks/ru/library/learning-content-mgmt/index.html>

Refleader.ru [Электронный ресурс] – Учебный процесс с использованием электронных учебников и электронных пособий – Режим доступа: <http://refleader.ru/yfsujgugotr.html>

Библофонд [Электронный ресурс] – Электронная библиотека студента – Режим доступа: <http://www.bibliofond.ru/view.aspx>

Allbest.ru [Электронный ресурс] – Разработка электронного учебного пособия – Режим доступа: <http://otherreferats.allbest.ru/programming>

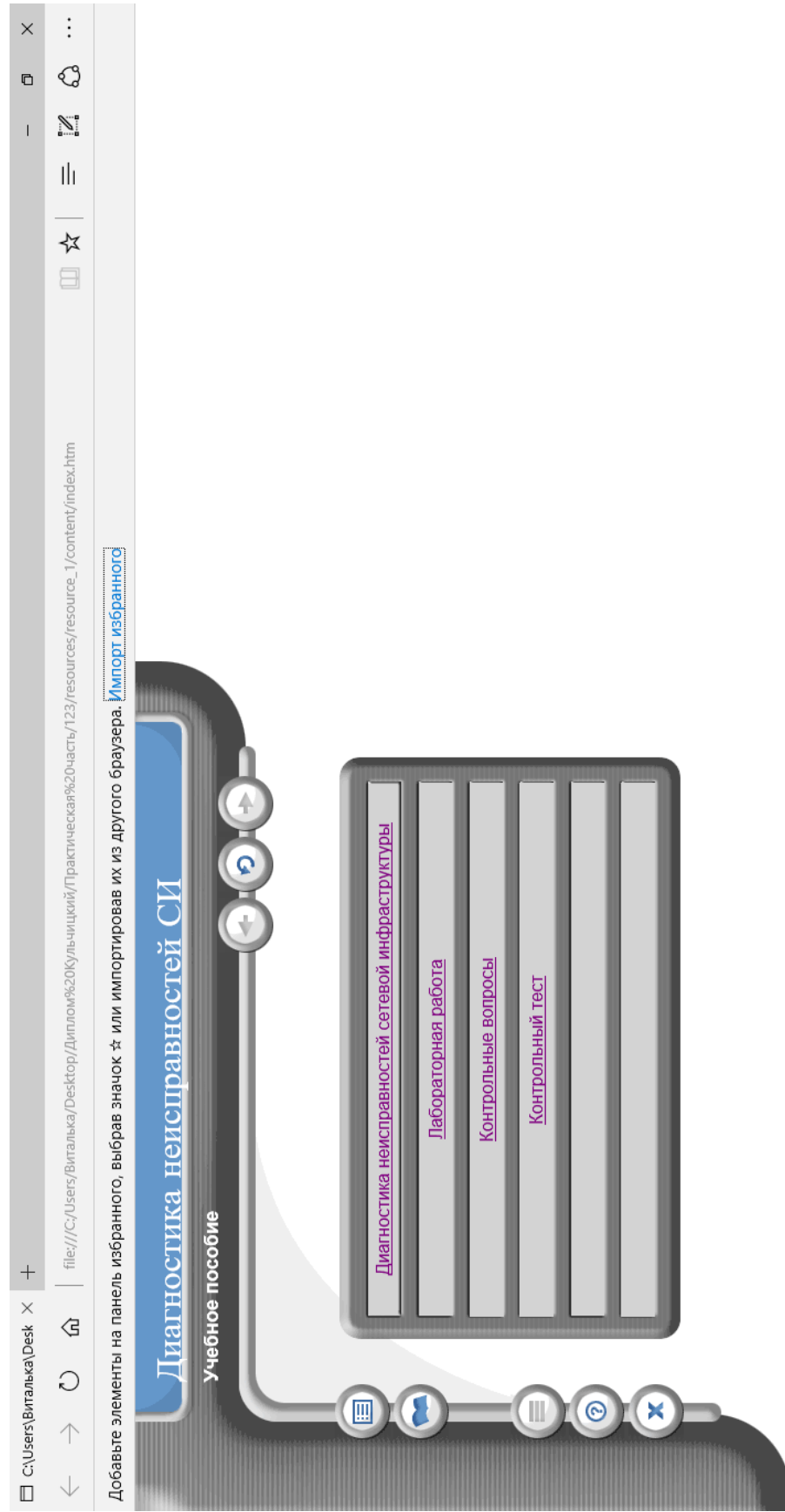
Информационные технологии [Электронный ресурс] – Режим доступа: <http://seti.ucoz.ru/>

Инфра Менеджер Документирование сети и кабельный журнал [Электронный ресурс] – Режим <http://www.inframanager.ru/functionality/documentation-of-the-network/>

Талисман группа компаний [Электронный ресурс] – Режим доступа: <http://www.talco.ru/index.htm>

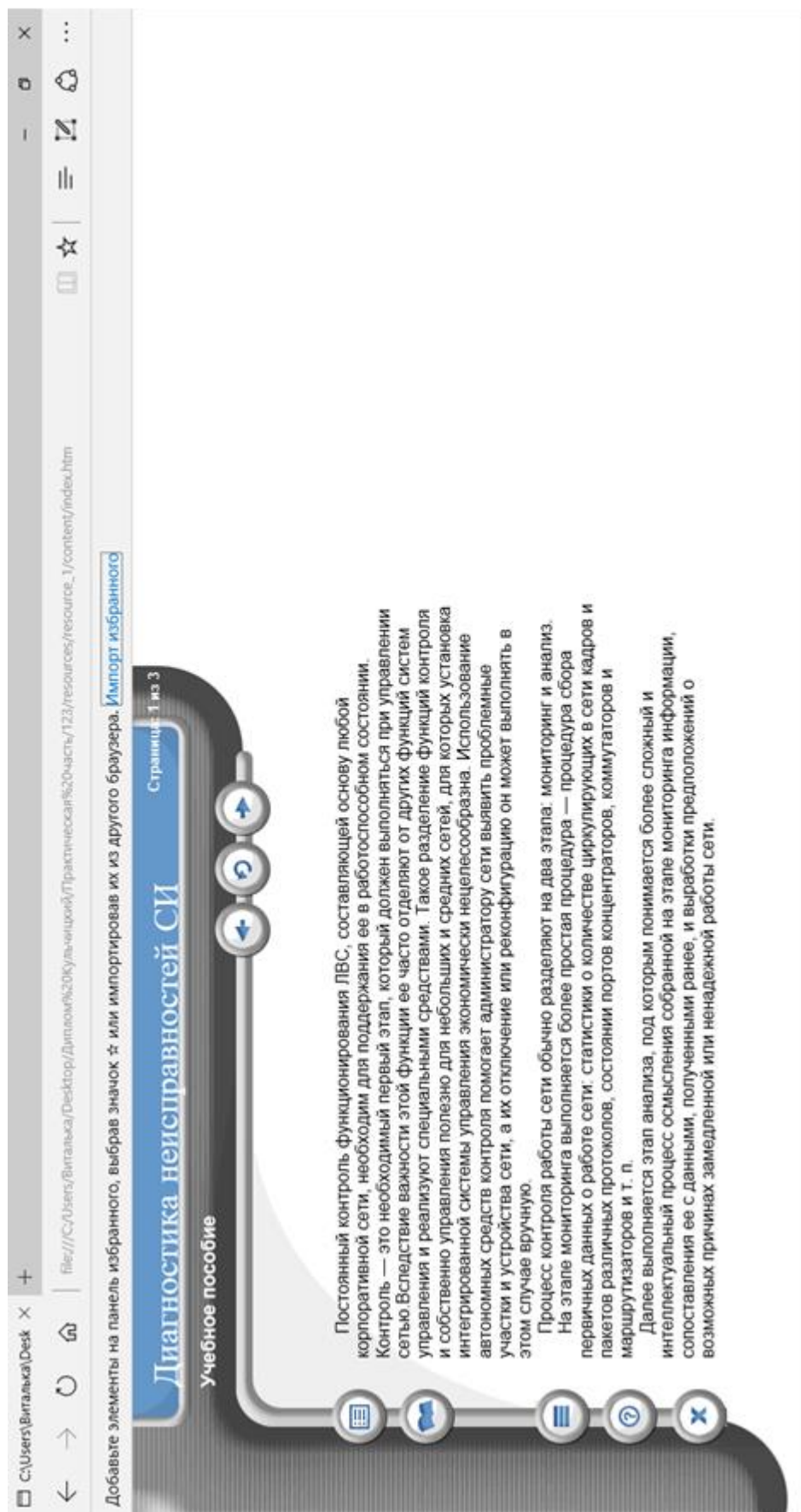
ПРИЛОЖЕНИЕ А

Главное меню учебного пособия



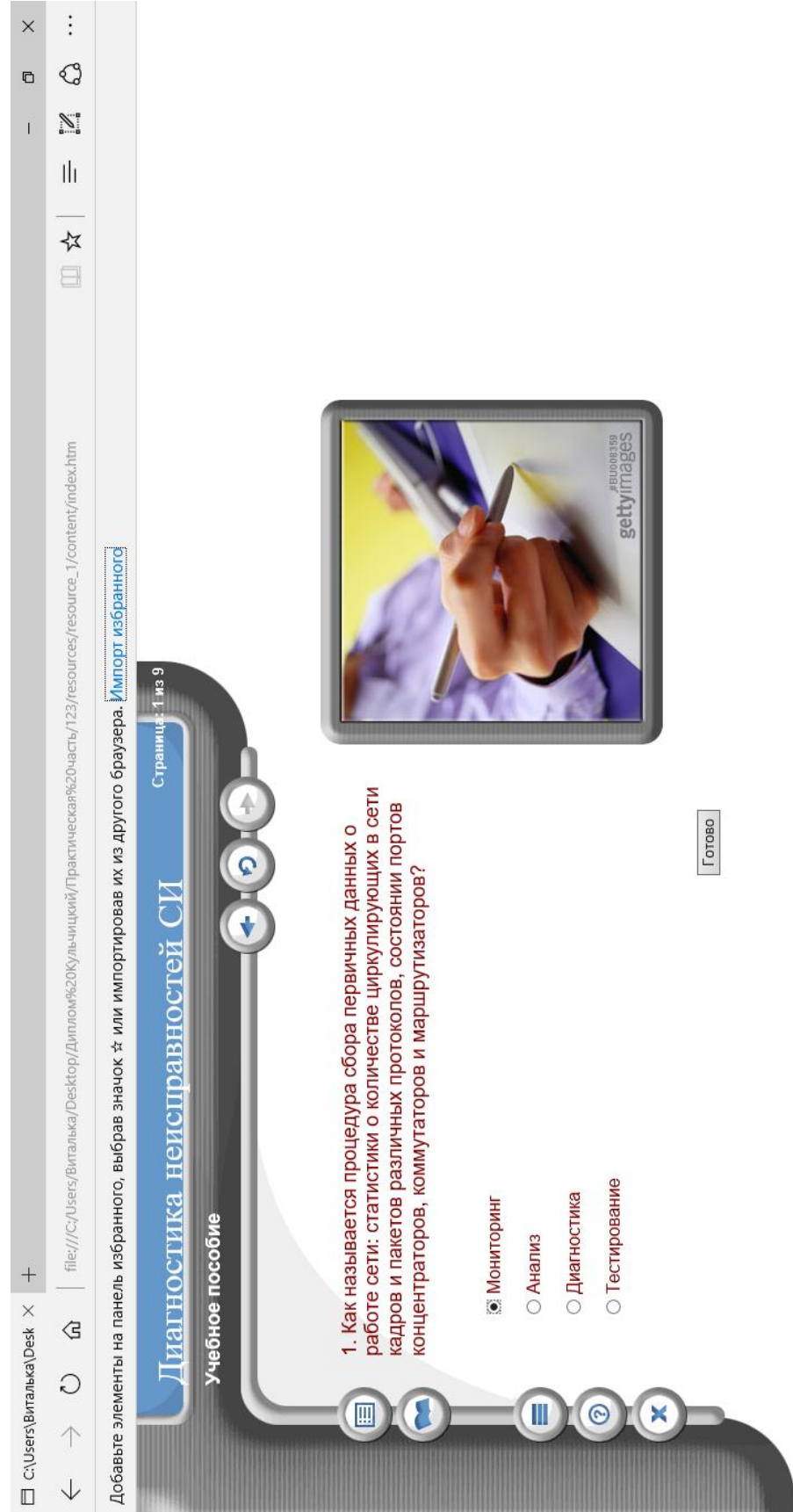
ПРИЛОЖЕНИЕ Б

Материал учебного пособия



ПРИЛОЖЕНИЕ В

Тесты учебного пособия



ПРИЛОЖЕНИЕ Г

Итоги теста обучаемого

С:\Users\Виталья\Desktop

+

←

→

↺

↻

🔍

🌐

🔖

☰

🔍

🔖

🔗

⋮

file:///C:/Users/Виталья/Desktop/Диплом%20Культуличий/Практическая%20часть/123/resources/resource_1/content/index.htm

Добавьте элементы на панель избранного, выбрав значок ☆ или импортировав их из другого браузера. [Импорт избранного](#)

Диагностика неисправностей СИ

Страница 9 из 9

Учебное пособие

⏮ ⏪ ⏩ ⏭

📋 🌐 📄 📖 📑

Экзамен	Вопрос	Я ввожу	Правильный ответ	Ответ студента	Результат
ex1	ex1o1q14	C	1	1	Правильный
ex1	ex1o1q15	C	3	3	Правильный
ex1	ex1o1q16	C	2	2	Правильный
ex1	ex1o1q75	C	1	1	Правильный
ex1	ex1o1q76	C	{1,6}	{1,6}	Правильный
ex1	ex1o1q78	F	netstat	netstat	Правильный
ex1	ex1o1q77	F	ping	ping	Правильный
ex1	ex1o1q79	F	tracert	tracert	Правильный

Ваша окончательная оценка: 100%

✓ Вы прошли экзамен